The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/0263-7472.htm

Risk management in facility management for data centres: status and deficits

Juergen Bieser
Faculty of Civil Engineering,
Bauhaus-Universität Weimar, Weimar, Germany
Björn-Martin Kurzrock
Faculty of Civil Engineering,
Technische Universität Kaiserslautern, Kaiserslautern, Germany, and
Ritika Batra
Faculty of Civil Engineering,
Bauhaus-Universität Weimar, Weimar, Germany

Received 30 November 2019
Revised 6 December 2019
Accepted 6 December 2019

Abstract

Purpose – Data centres (DC) serve as critical infrastructure and require a sustainable and uninterrupted building operation. Effective risk management (RM), as a component of enterprise RM (ERM), is the basis for secure DC operations. The purpose of this paper is to determine, whether holistic and integrated RM solutions already exist or what they might look like.

Design/methodology/approach – A literature review of laws, norms, standards, methods and certifications combined with transcribed paper and pencil expert interviews with DC, facility service companies and consulting firms has been conducted. The study also investigates RM practices of 23 large international DC and facility service companies.

Findings – Results of literature research and intensive interviews with experienced DC experts, covering the entire life cycle of buildings, indicate that there are no holistic and integrated RM practice applications for DC on a sound academic basis.

Practical implications – Findings suggest that there is a need for developing a holistic and integrated RM framework for DC. This paper is a contribution to the expansion of ERM research and can be very valuable for builders and operators. The results of this research form the basis for the development of a structured RM framework for DC that improves performance.

Originality/value – The study allows professionals to understand the operational state-of-the-art of RM in critical environments and shed light on the wide spectrum of conceptualities and definitions.

Keywords Risk management, Building life cycle, Facility services, Digitalization, Data centres

Paper type Research paper

1. Introduction

Data centres (DC) are a structure or a group of structures intended for the interconnection as well as the operation of information technology (IT) and network facilities that provide data storage, processing and transmission services (DIN EN 50600:2016, 2016). Such IT infrastructure is supported by complex technical facilities like power supply, cooling and monitoring systems, in order to ensure service availability along with high levels of reliability, security and environmental control (Kunbaz and Bieser, 2018). Studies by IT analysts have shown that the average cost per minute of IT equipment downtime is approximately $9,000, depending on the industry in which the company operates and the average reported incident length is 95 min, resulting in average costs per incident exceeding $850,000 (Ponemon Institute, 2016). This illustrates the enormous potential impact of failures in the operation and maintenance of the DC infrastructure.

Due to the rapid digital transformation in our societies, the demand for data is ever-growing. Global DC internet protocol (IP) traffic is expected to triple over the next five years. Overall, DC

0263-7472
DOI 10.1108/PM-11-2019-0068

IP traffic will probably grow at a Compound Annual Growth Rate of 25 per cent from 2016 to 2021 (Cisco, 2018). Given this, DC worldwide are being built in ever-shorter cycles. The factor of time and money, combined with high demands regarding the quality of execution, places distinct requirements on the constructors and owners of these special properties as well as on service providers. Poor risk management (RM) in DC environments can foster a wide range of consequences including increased downtime and disruption to essential services. Costs of system unavailability include a loss of capacity and costs of defects and delay as well as a loss of brand damage and insurance deductibles due to lack of mitigation, legal considerations, etc. (Asset Insights, 2013). Tweeddale (2003) adds a moral and ethical dimension for managing risks to avoid injuries and environmental disasters.

The primary objective for facility management (FM) in DC, therefore, is to ensure sustainable and uninterrupted operation of supply systems to prevent losses, in particular of data and profits. To ensure this, the risks must be identified at an early stage and throughout the entire life cycle (LC) of a DC. The definition of the LC phases of buildings varies in literature. According to ISO 15686-1:2011 (2011), there are four LC phases: acquisition, use/maintenance, renewal/adaptation and disposal. Furthermore, detailed definitions can be found in literature (GEFMA 100-1:2004, 2004; DIN EN 15978:2011, 2011; EPA, 1993). All LC models can be traced back to a common basic principle. An initial phase (concept/design), a use phase (operation) and a final phase (disposal). The LC share of the building operation use phase of DC is approx. 80 per cent (Kunbaz and Bieser, 2018).

All activities in a company that deal with opportunities and threats (risks) must be subjected to RM (Gleißner, 2016). The regulation of companies now strictly calls for the implementation of (rather sophisticated) RM systems. In particular, Basel III and Solvency II stand as directives in the European Union law and aim to harmonise EU bank and insurance regulation (O'Shea and Krischanitz, 2013). Since DC serve as critical infrastructure, RM standards for the operation of DC are likely to evolve or even be required by law in the near future.

2. Literature review

Reviewing the literature regarding RM, an extensive body of different models and research fields was found. Pakhchanyan (2016) reviewed 279 academic papers on operational RM in financial institutions and highlighted research gaps for future research on the impact of operational loss events. Ennouri's (2013) RM literature review described definitions and methods on supply chain risks as a basis for future research in the industrial sector. Bromiley *et al.* (2015) argued that enterprise RM (ERM) offers an important new research domain for management scholars and also point out, that further holistic RM research will contribute the fundamental understanding in management scholarship and to important practical problems. The review paper from Yongrok *et al.* (2016) identified the most cited academic papers in the field of ERM with the following conclusion: "[…] Even if the elements of risks are complicated and diverse, it is preferable for individual companies to integrate several methods for similar contents of risks and compare these with several other alternative methods. Even if there is no generalized version of ERM, it is feasible for professional experts to search, measure, monitor, and manage all the contents and methodology-specific risks by systematic integration of the diverse approaches and by comparing the possible outcomes with the alternative approaches […]". Tixier *et al.* (2002) reviewed 62 risk analysis methodologies of industrial plants and came to the conclusion that there is not only one general method to deal with the problematic of industrial risks.

The classification of the research area RM in DC for FM can be assigned as a part of ERM from the author's point of view. In the literature, there are already several publications on the combination of FM and RM (Kucera and Pitner, 2013; Bockstefl and Redlein, 2012; Keith, 1992). The paper by Zheng *et al.* (2016) defines an RM system which is based on a management framework with a focus on the control of compliance risk and operational risk. The results of this research rest on the ERM of COSO[1] and focus mainly on IT. FM is a part of the holistic investigation, but it is treated very superficially. The authors Levy M. and Raviv D. (2018) investigated in their research work the RM in DC including FM aspects. There outcome is a scorecard for considering DC site risks. These results investigate the combined topics RM+DC+FM and thus form a good basis for further research. No further academic results could be found in the literature.

3. Aim, methodology and scope of research

RM in FM, in particular for DC, is a rather new issue that is gaining more and more importance as DCs continue to grow in number and size (Marzuki and Newell, 2019). The aim of this research is to compare current laws, norms, standards and methodologies for RM of DC and to make recommendations for the development of a holistic and integrated RM for this complex type of asset. Therefore, this paper addresses the following research questions (RQ):

RQ1. How can laws, norms, standards, methods and certifications in DCs currently applied to RM be related?

RQ2. What could serve the basis of a future holistic and integrated RM?

Along with the literature review, this paper examines company profiles of DC and FM companies, laws, norms, standards and methods and qualitative methods in the form of extensive expert interviews with experienced employees of various companies who cover the complete LC of buildings. The paper continues with the aim of answering the two RQ and thus closing the research gap.

Table I reflects the largest DC operators and facility service firms worldwide, which have been reflected in empirical analysis. DC companies[2] have aggregated annual revenues of $950bn. The revenues of the facility service companies exceed $220bn.

The information in Tables I and V was researched using company profiles and publications. International FM and DC companies were checked for implemented management certifications. Six companies (JLL, Microsoft, IBM, Digital Realty, Dussmann and Apleona) also contributed supplementary interviews which were conducted by telephone with company representatives and took between 10 and 20 min. The intention was to verify the results of Tables I and V by random sampling interviews and these were transcribed and confirmed by the interview partners.

In all, 11 extensive expert interviews with company representatives in the field of DC operators, FM and consultancy companies covered the whole LC of buildings. These internationally experienced experts have been working in the DC industry for more than 10 years and are very familiar with the LC of buildings as well as the practices used. The aim of these extensive discussions was to uncover representative aspects. The duration per interview was between 1 and 2 h. The interviews were semi-structured with the aim of recording qualitative (interpretation) and quantitative (measurement) aspects (Atteslander, 2010). As such, they were based on preparatory questions in arbitrary order, and information arising from the conversation was recorded and followed up. The results from the interviews are summarised in Section 4.5 and the details can be found in Table AI.

4. Results and discussion

In the following Sections 4.1–4.3 definitions of laws, norms, standards, methods, as well as the current status of the deficits/gaps, are examined. Section 4.4 defines and elaborates on the concept of integrated RM for DC. The certifications used in practice already take components of RM into account. Section 4.5 examines the results of the two RQ through intensive discussions with experts. From the author's point of view, there are significant

No.	Company	Sector	Headquarter	Scope	Annual revenue (US$)
1	Apple	IT	Cupertino, USA	International	265.6bn (2018)
2	Amazon	Online Trading	Seattle, USA	International	232.9bn (2018)
3	Digital Realty	Data Centres, Real Estate Investment Trust (REIT)		International	3.0bn (2018)
4	Equinix	Data Centres, Real Estate Investment Trust (REIT)	Redwood City, USA	International	5bn (2018)
5	Facebook	Social media/networking	Menlo Park, USA	International	55.8bn (2018)
6	Global Switch	Data Centres	London, UK	International	Not defined
7	Google	IT	Mountain View, USA	International	136.2bn (2018)
8	IBM	IT	Armonk, USA	International	79.6bn (2018)
9	KDDI	Telecommunication	Tokyo, Japan	International	42.6bn (2015)
10	Microsoft	IT	Redmond, USA	International	110.4bn (2018)
11	NTT Data	IT	Tokyo, Japan	International	19bn (2017)
12	Apleona	FM/Real Estate	Neu-Isenburg, Germany	International	2.84bn (2015)
13	CBRE	FM/Real Estate	Los Angeles, USA	International	14.2bn (2017)
14	Caverion	FM/Plant Engineering	Kulmbach, Germany	International	2.5bn (2017)
15	Dussmann	FM	Berlin, Germany	International	2.5bn (2017)
16	Engie/GDF Suez	FM/Plant Engineering	La Défense, France	International	73.9bn (2017)
17	ISS	Integrated Services	Copenhagen, Denmark	International	11.9bn (2018)
18	JLL	Services	Chicago, USA	International	16.3bn (2018)
19	Piepenbrock	FM	Osnabruck, Germany	International	0.576bn (2015)
20	Strabag	Construction/FM	Vienna, Austria	International	15.3bn (2017)
21	Spie	Multi-Services	Cergy, France	International	7.6bn (2017)
22	Sodexo	Catering, FM	Issy-les-Moulineaux, France	International	23.2bn (2018)
23	Vinci	Construction/FM	Rueil-Malmaison, France	International	49.5bn (2018)

Source: Own research

Table I.
DC companies and facility service companies included in empirical analysis

gaps or deficits that can be closed by the creation of an RM framework, taking into account the recommendations from the experts combined with further research.

4.1 Facility management for data centres

As Atkin and Brooks (2015) point out there is no universal approach for managing facilities. This is also reflected by a range of international and country-specific norms and standards, as well as general FM definitions (see Table II). German FM Association (GEFMA, 2019)

Norms and standards	Description	Year
DIN EN 15221	Facility management	2007
DIN 32736	Building management	2000
GEFMA 100-1	FM fundamentals	2004
GEFMA 100-2	FM scope of service	2004
ISO 41001:2017	FM management systems	2017
ISO 41011:2017	FM vocabulary	2017
ISO 41012:2017	FM guidance on strategic souring and the development of agreements	2017
ISO 41013:2017	FM scope, key concepts and benefits	2017
VDI 6009:2002	Facility management	2002

Source: Own research

Table II.
Facility management, international norms and standards

defines FM as a result-oriented management domain dedicated to facilities and facility services[3]. FM is to ensure that premises are managed with maximum efficiency through planned, steered and controlled facility processes, in order to meet the basic needs of people in a workplace, support core business processes of an enterprise and increase the return on capital. According to DIN EN 15221-1:2007 (2007), FM covers and integrates a very broad scope of processes, services activities and facilities. The new ISO 41012:2017 (2017) standard offers guidance on sourcing and development of agreements in FM. Since FM covers the whole LC of buildings it must add to the normative and strategic guidance with appropriate authority (GEFMA, 2019). Clearly, all this applies to DC as for any other property type. Above all, DC are pieces of critical infrastructure with a high degree of technology and growing user demands.

According to IFMA (2019), FM encompasses multiple disciplines to ensure the functionality of the built environment by integrating people, place, process and technology. This includes the on-going analysis and optimisation of cost-relevant processes on structural and technical installations, equipment and services that do not belong to the core business of an enterprise.

In an "ideal" DC, only two organisations exist: the primary IT service provider and the secondary facility service provider. Primary activities are related to the operation of IT systems. Currently, these services belong to the core business of the customers and include, e.g. IT hardware planning and installation, server hosting and operations and IT security. Usually, secondary services include the design, operation and maintenance of all power supply systems, all building services systems, emergency and fire-safety systems, etc. The fewer the interfaces between primary and secondary services, the lower are the communication and "management efforts". Thus, a bundling of facility services may contribute to minimising any risk involved in operating a DC (Bieser and Menzel, 2017).

International norms and standards related to FM are technical documents designed to be used as a rule, guideline or definition created by recognised organisations in order to set specific criteria for products, processes, operations, services, etc., as well as to create a common benchmark where performance can be demonstrated and measured.

The following paragraphs provide an overview of the existing standards. DIN norms are the standards based on proven results of science, technology and experience and are developed by the German Institute for Standardisation on a national level. The International Organisation for Standardisation (ISO) also issues European standards (EN) that almost cover all aspects related to FM. GEFMA (2019) is involved in standardisation work in the area of FM and intends to create standards and develop guidelines for ensuring quality and safety in FM. VDI (Association of German Engineers) creates technical regulations and guidelines that contain state-of-the-art recommendations and rules related to technical FM. However, VDMA (Mechanical Engineering Industry Association) is the largest industrial association in Europe, which publishes VDMA standard sheets that specify standardisation procedure for mechanical engineering. DIN EN 15221-2 norm and GEFMA 100-1:2004 (2004) guideline describe general FM standards and interfaces between customers and service providers. GEFMA 100-2:2004 (2004) attributes the range of services over the whole LC of buildings and infrastructure and describes how resource optimisation should be taken into account as early as in the design phase. DIN 32736:2000 (2000) comprises all services regarding the operation and management of buildings including structural and technical facilities. Given that all of the aforementioned (national) norms and guidelines were released between the years 2000 and 2007 and do not relate to a particular property type, it is no wonder that DC get no mention there.

The international ISO 41001:2018 standard also presents FM and the related requirements independent of the industry. ISO 41012:2017 (2017) and ISO 41013:2017 (2017) regard FM from a strategic point of view and present general key concepts and benefits. VDI 6009:2002 (2002) gives guidance on the implementation of building management for multiple properties and on introducing Computer Aided FM systems.

From literature, limited research results (Levy and Raviv, 2018) could be found concerning FM in DC either. However, a European norm, DIN EN 50600:2016 (2016), was released between 2012 and 2018. This norm consists of four chapters with ten approved sections, covering all areas of DC infrastructure (Table III). Section 3.1 (DIN EN 50600:2016, 2016) deals with operational content and specifies processes for the management and operation of DC (Figure 1). The focus is on operational processes to improve resilience, availability, RM, risk avoidance, capacity planning, security and energy efficiency. In addition to a definition of terms, basic operational requirements are defined. A view on optimal operation during the LC of DC is included in Sections 2.1–2.5 of the norm. The norm recommends that the FM operator be extensively involved in acceptance tests in order to document the successful or faultless commissioning of the technical supply facilities, which constitutes an important step to minimise operational risks. Also, the basics for the introduction of operational processes and management processes are described. However, the norm deals only superficially with RM.

The ISO/IEC TS 22237 series is an internationalised version of DIN EN 50600:2016 (2016), which focusses only on technical specifications (TS) rather than international perspectives because this was the quickest way of publishing them. The reason behind this is that the USA and Japan felt that DIN EN 50600:2016 (2016) was so important that they sought a fast implementation (Gilmore, 2019).

In sum, DIN EN 50600:2016 (2016) has successively developed as an EN, which is in part being further developed into an international standard, ISO/IEC TS 22237. One part,

Table III. DIN EN 50600, structure

Norm	Description	Year
EN 50600-1	General concepts for design and specification	2018
EN 50600-2-1	Building construction	2012/14
EN 50600-2-2	Power distribution	2014/16/18
EN 50600-2-3	Environmental control	2013/18
EN 50600-2-4	Telecommunications cabling infrastructure	2014/15
EN 50600-2-5	Security systems	2014/16
EN 50600-3-1	Management and operational information	2014/16
EN 50600-4-1	Key performance indicators	2016/17
EN 50600-4-2	Power usage effectiveness	2016/17
EN 50600-4-3	Renewable energy factor	2016

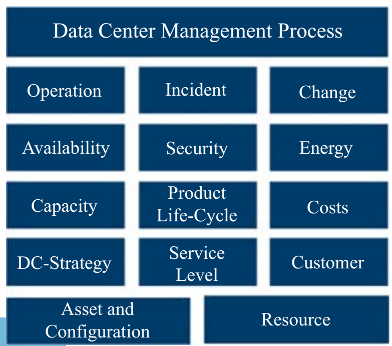


Figure 1. DIN EN 50600-3-1, DC management processes overview

DIN EN 50600-3-1:2016 (2016), refers to operation. The necessary basics are defined briefly and concisely and are to be designed and implemented in particular by the FM operator.

In all of the norms and guideline series mentioned, RM for buildings and infrastructure is specified as a task in which the FM operator is at least involved. The FM operator is strongly involved in the LC of a building and may take over a central role in the RM for DC.

4.2 Risk management for data centres

RM systems define all principles, processes, methods, responsibilities and designations for implementing the RM of an organisational unit (ISO 31000:2018, 2018). The RM of an organisational unit includes almost all risk-related activities of the organisational unit or company (Wälder and Wälder, 2017). There are several risk process models in the literature (e.g. Hopkin, 2017; Diederichs, 2018; Romeike, 2018) that differ slightly in some details. The lowest common denominator is linked to a cycle of four phases: risk identification, risk analysis and evaluation, risk control and risk monitoring. All of the phases need to be operationalised. ISO 31000:2018 (2018) refers to the first two phases as risk assessment and to the following as risk treatment.

It is pointed out in DIN EN 50600-1 that a loss of redundancy of the technical building equipment increases the risk of failure. Furthermore, it is recommended that a risk assessment be carried out at least once a year or in the event of significant changes in the technology or infrastructure of the DC. There is no specific recommendation for action on how to carry out the risk assessment but the reference is made to the generic standard IEC 31010:2009 (2009)[4], which provides guidance on the selection and application of systematic techniques for risk assessment. The other sections of DIN EN 50600:2016 (2016) also contain requirements for carrying out risk analyses. These include site factors, fire protection, air conditioning and physical security. In this respect, there are no specific recommendations on how risk assessments should be carried out.

The aim of risk control is essentially to minimise risks. In the case of buildings and infrastructure, risk avoidance means to pay attention to, for instance, location factors and eventually refrain from an investment. A reduction of risks is possible through the development of a robust technical infrastructure, i.e. redundant or high-quality plant components, as well as the introduction of secure processes. Contractual regulations can be used to shift or limit risks. These reductions are to be achieved through effective risk controlling. The remaining residual risk must either be insured or has to be accepted.

Generally, there is a distinction between normative, strategic and operational RM (e.g. Hopkin, 2017; Chapelle, 2019; Wengert, 2013). On this basis, strategic RM refers to the embedding in the entire company and focusses on long-term risks. The operational RM relates to the handling of specific risks in day-to-day business.

Denk and Exner-Merkelt (2008) divide the development of RM in seven phases: insurance management and compliance, risk assessment, risk/return network and securing business success targets, risk status management, RM growth orientation, holistic strategic RM and value-oriented RM strategy. This strategic orientation is assigned to Corporate RM. Meyer (2013) describes an RM set for engineering that can also be applied to FM. This consists of the components: reliability engineering, risk communication, risk treatment, risk reduction, risk assessment, safety management system development, legislation and regulations, risk climate and risk culture, economic issues of risk, learning from accidents, business continuity planning, safety, maintenance management and psycho-social aspects of risk.

This development shows the complexity of today's RM, which is no longer just about assessing individual operational risks, but about a holistic assessment within the company. Table IV provides an overview of the relevant laws, norms, standards and methodologies of RM.

DIN EN 50600:2016 (2016) recognises the central role of FM for RM in DC, but only marginally treats RM without giving any specific recommendations for carrying out

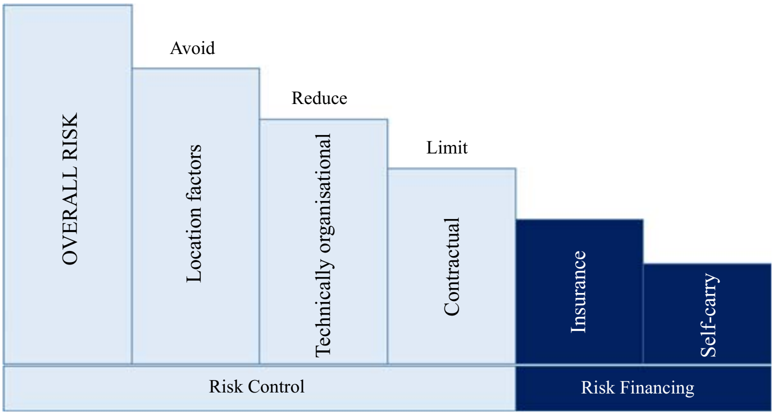
Table IV.
Risk management – laws, norms, standards and methodologies

S. No.	Category	Risk management (RM) Laws, norms, standards, methodologies	References
1	Laws	2,000 laws and 3,500 regulations in Germany such as KonTrag, Banking Act, Basel II and III, Solvency II and others	Romeike (2018)
2	Management methods, standards and guidelines	BSI, ISO 17779, ISO 22301, COSO-ERM, AS/NZS 4360, ONR 49000:2014 (2014) ff, ISO 31000 ff, FERMA	Romeike (2018), Wiggert (2009)
3	Risk identification methods	Analysis of Strategic Planning, Assumption Analysis, Survey Analysis, Brainstorming, Brainwriting, Business Impact Analysis, Check List, Documentation Analysis, Expert Survey, Fault Tree Analysis, FMEA, Hazard and Operability Studies (HAZOP), Ishikawa, KJ Method, Life Cycle Cost Analysis, Markov Analysis, Mind Mapping, Pondering, Pre-Mortem Technique, Organisational Analysis, Pert, Risk Registers, Social Network Analysis, Synectics, SWOT Analysis, Scenario Analysis, World Café, Workshop, 6-3-5 Method	Romeike (2018), Alfen *et al.* (2010), Huth *et al.* (2017), Hopkin (2017)
4	Risk analysis and evaluation methods	Qualitative: relevant decision, risk list, Failure Mode and Effects Analysis (FMEA), Qualitative assessment of probability of occurrence and scope Qualitative-Quantitative: Fault Tree Analysis (FTA), Expert Assessment/Survey, Delphi Method, Risk Map Quantitative: Quantitative assessment of probability of occurrence and scope, correction procedure using risk premiums, ABC analysis, Equi-Risk-Contour method, scenario method, Quantitative description of risks by means of distribution functions (stochastic and heuristic) Overall Risk Rating: Impact Analysis, Pression and Correlation Analysis, Variance-Covariance Model, Probalistic Event Analysis (PEA), Scoring Models, Overall Risk Assessment Scenario, Sensitivity Analysis, Historical Simulation, Monte Carlo Simulation, Fuzzy Logic, Artificial Neural Networks (KNN)	Alfen *et al.* (2010), Hopkin (2017)
5	Risk control methods	Decision table, decision tree method, utility value analysis, simulation method	Alfen *et al.* (2010), Hopkin (2017)
6	Risk monitoring methods	Balanced Score Card Plus (BSC Plus), Balanced Chance and Risk Card (BCR Card), Earned Value Analysis, Risk Trend Analysis, Variance Analysis	Alfen *et al.* (2010), Hopkin (2017)

Source: Own research

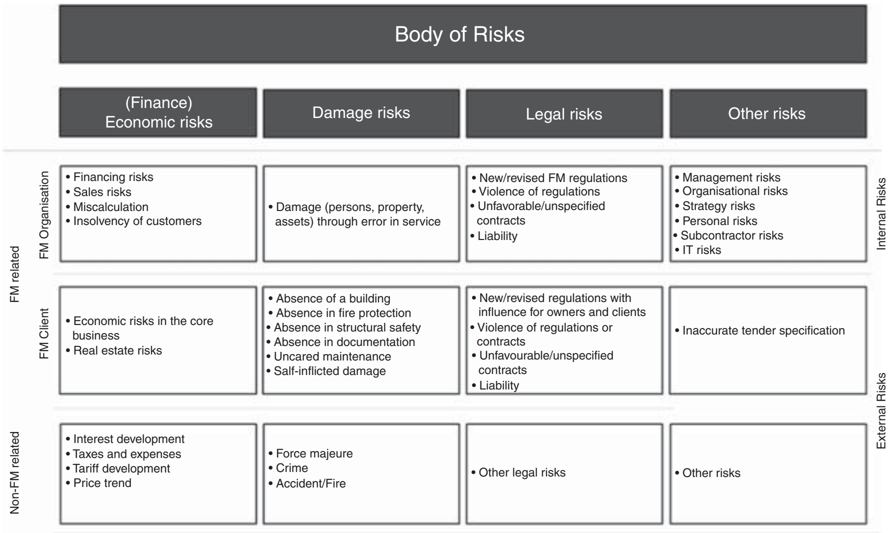
risk assessments. While the overall presentation remains rather vague, there are at least many indications as to which criteria should be subjected to a risk assessment. For instance, in the context of change management[5] processes, a risk assessment of the effects is deemed necessary for every change in a DC (e.g. replacement of equipment or performance of maintenance work). For changes that cannot be successfully implemented, a recovery plan is required. Change requests shall be approved by a committee prior to execution (Figure 2).

GEFMA 192:2013 (2013) classifies risks in the operational business where FM processes are implemented (e.g. DC) into four main categories: financial/economic risks, risk of damages (operational failures, human error, etc.), legal risks and other risks that are mainly related to management and organisational risks. The body of risks in FM with regard to internal and external factors, customers and their specific relevance is shown in Figure 3.



Source: Adapted from Romeike and Hager (2013)

Figure 2.
Risk control in practice



Source: GEFMA 192:2013 (2013)

Figure 3.
Body of risks in FM

4.3 Integrated RM in FM: reliability, availability, maintainability and safety (RAMS)

Similar to the definition of RM, there are also different derivations and definitions for integrated RM. A magazine of the RM, International Affairs Section of the German Federal Office for Civil Protection and Disaster Assistance (Katastrophenhilfe, 2018), defines Integrated RM as a strategic approach, which pre-disposes of potentially damaging events for the population in the run-up to potential disasters. This approach focusses on emergency planning in critical situations. In the insurance sector, the definition of this term has a fundamentally different meaning and refers to procedural monetary optimisation approaches.

With regard to buildings and infrastructure, the international ISO 31000:2018 (2018) standard is the most extensively involved with the integration of RM into corporate structures from the authors' point of view. Wälder and Wälder (2017) object that RM systems cannot be certified according to ISO 31000:2009, because the standard does not contain any direct requirements, but only principles and their procedures; this still holds for ISO 31000:2018: (2018). The Austrian standard ONR 49000:2014 (2014) has developed into the basis for the practical implementation of the ISO 31000:2018 (2018) standard, in particular for Germany, Austria and Switzerland. Similarly, the British standard BS 31100 explains how to develop and implement the ISO standard into practice.

Still, with the continuous development of FM as well as the increased legal requirements and a holistic LC assessment of buildings and infrastructure, RM has evolved from originally purely economic activity to an important integrated management function. In (technical) FM and the operation of complex facilities, the variables RAMS play important roles:

(1) Reliability is defined as the capability of an item to perform a required function under given circumstances for a given interval (IEC 60050, 191-02-06).

(2) Availability is the ability of a unit to be able to perform a required function under given conditions, at a given time or during a given time interval, on condition that the required external tools are provided (IEV 191-02-05). This means availability of 100 per cent for installations that are available 24 h a day (8,760 h) on 365 days a year.

(3) Maintainability is a measure of how quickly and effectively the normal operation can be restored after a fault or an interruption (ITIL v3) (ITIL, 2017).

(4) Safety can be classified into three categories: personal protection, equipment protection and environmental protection and is defined as not involving risk (Stapelberg, 2009).

For an effective RM as outlined above, the aim is to identify, evaluate, control and monitor all risks across the four areas as far as possible so that uninterrupted plant operation can be ensured. Failure mode, effects and criticality analysis (FMECA) is a fundamental systematic analysis tool to identify failure modes, their causes and consequently their fallouts on the system function (Ben-Daya *et al.*, 2009). Identified risks based on the factor's severity, occurrence and detection are ranked in risk priority numbers before risk mitigation measures lead to the reduction of operational risks. Reliability, availability and maintainability (RAM) modelling is a methodology used to predict asset performance over a defined time span. Both methods can be combined to an FMECA/RAM(S) analysis to identify risks over the entire LC of buildings or infrastructure (Kunbaz and Bieser, 2018).

Section 4.2 already showed deficits that currently exist in the area of RM for DC. Further results from the literature research and expert interviews in Section 4.5 confirm the high demands on the uninterrupted operation of DC. The main criteria for reliable operation appear to be the avoidance of human errors and the early detection of technical faults. In this context, there are extensive requirements for documentation management and compliance with processes.

4.4 Integrated RM for data centres

FMECA can also be adopted to perform risk analyses in the area of the technical infrastructure of DC. RAM modelling may provide a statistical basis for evaluating the impact of proposed changes obtained from the FMECA in terms of DC availability and reliability, offering a strategic view of how various systems perform over longer time spans (Kunbaz and Bieser, 2018).

With regard to FM in DC, risks mainly focus on damages/losses and related legal aspects. As for the management of buildings and infrastructure in general, all of the RAMS criteria apply. In operation management, the human factor (still) plays an important role in the reliable, resilient and economic operation of complex facilities. In the literature, different views on the human factor are found. In particular, the VDI 4006:2003 (2003) guideline offers various methods to assess human reliability, speaking of methods for quantitative assessment of human reliability (HRA). The task of the HRA is to:

- qualitatively analyse human actions, thus, to identify possible errors in actions, identify weak elements, which provide the basis for appropriate countermeasures; and
- quantify the reliability of human actions, which for instance allows for assessing the effectiveness of remedial or countermeasures (e.g. a safety gain) within the overall system.

The Uptime Institute (Onag, 2016) stated that 70 per cent of DC outages are caused by human error. Human error is considered a part of everyday functioning and it is expected that people occasionally make errors. In fact, many research studies reflect on the importance of the human factor when operating complex facilities (e.g. Hooper and O'Hare, 2013; Guicang, 2014; Onag, 2016). It is the main goal of maintenance in DC to ensure reliable operation and to detect any risks and failures before they arise. An early literature review by Dhillon (2002) shows the importance of human error in engineering maintenance. Maintenance errors can occur as a result of poor design factors including issues involving equipment, maintenance, work layout and difficulties faced by workers like improper working tools, fatigue and environmental factors, such as humidity, lighting, temperature, etc. Finally, improper training, the use of obsolete maintenance manuals and the lack of relevant experience contribute to a high number of maintenance errors. Improvements could be achieved by taking these factors into account by hiring workers with more experience and suitability for their environment, providing emotional stability and leading to less fatigue, improved teamwork and better morale.

Current DC operation and maintenance strategies aim to deliver extremely high reliability of DC and their support systems (power supply, cooling, lighting, etc.) by installing redundant engineering systems to prevent service outages. However, this approach requires substantial additional investment in the availability of redundant systems and components, further increasing the complexity of service systems in modern buildings. This increased complexity can even lead to undesirable consequences of further increasing operational failures.

The Tier-Standard developed by the Uptime Institute (Uptime, 2019) has established itself worldwide for determining the reliability of DC. This standard describes the design of building services installations on the basis of four main classifications. Tier 1 means that there is no redundancy of the building services systems so that a failure of one system can lead to a complete failure of the DC. On the other hand, Tier 4 refers to the maximum reliability with fully fault tolerant building services equipment. In practice, Tier 3 concurrently maintained that DC are very common, with Tier 3 tolerating a maximum of 1.6 h of downtime per year, providing a cost/benefit ratio suitable for most applications. In practice, design flaws are identified based on regular reviews. This includes answering questionnaires and sampling plant schemes, followed by interviews with planners, planners and operators. This is a good example of a qualitative method for risk identification. Alternatively, it is possible to identify and analyse risks over the entire LC using quantitative methods such as a combined FMECA/RAMS.

Recent Uptime Institute survey results prove that a majority (80 per cent) of the respondents believe their biggest/most recent outage (for those who had suffered one) was "preventable". This result also suggests that the most common cause of problems lies in processes and practice, rather than architecture or equipment. But the survey also supports the view that cautious and careful design at the outset does reduce outages (Lawrence, 2018). In summary, it can be concluded that the implementation of an effective RM may prevent DC outages. The main causes of failures are human error, equipment failure and inadequate processes and procedures. However, an integrated RM approach is required for both international facility service and DC companies, in order to understand the full scope of risks associated with DC critical environment.

Companies opt for certifications in order to ensure sustainable compliance with the required criteria. A certification is a procedure for proving compliance with certain requirements, which are defined in a catalogue of criteria. This also includes conformity with norms and standards. According to DIN EN ISO/IEC 17000:2004 (2004), certification means the declaration of conformity by a third party with regard to products, processes, systems or persons. Assessment means the verification that the selection and verification activities and their results are appropriate and effective in relation to the fulfilment of the specified requirements by the object of the conformity assessment. On the one hand, the effort and costs for the introduction of these management systems are high. On the other hand, costs and risks can be reduced by introducing these systems. End customers who rent IT space or outsource services to the DC provider determine which management systems are absolutely necessary before signing a contract. Certification is generally limited in time and is renewed at regular intervals. In the follow-up audit, it is checked whether the company complies with the required criteria or continuously improves them.

The author(s) argue that both international facility service and DC companies have several management certifications as part of their core business, with RM indirectly involved and understood according to the respective certified party, whether they are facility service or DC companies. Identifying synergies on both sides may provide the basis for an integrated RM approach. Along with literature research, 23 large international DC and facility service companies were surveyed, and in-depth analyses of their official reports were performed.

Table V reflects the results of literature research and surveys of international companies. In some cases where the information could not fully be obtained, telephone interviews were conducted with company representatives.

The analysis shows that all 23 companies are ISO 9001 certified. This international standard employs the process approach which incorporates the Plan-Do-Check-Act cycle and risk-based thinking. The origins of ISO 9001 date back to the 1990s. The structure of the continuous improvement process has also been adopted by other international norms and standards. In five cases (highlighted in blue), the same management systems exist in companies. In 33 certifications (highlighted in orange), the management systems already contain partial requirements for RM.

Furthermore, it is evident that each company decides very individually for the implementation of management systems. Some of the companies surveyed deliberately refrained from external certification. In these cases, the company-specific terms are created and regularly checked internally. The companies orient themselves on selected norms, standards and guidelines and ensure compliance as well as continuous improvement through a best practice approach.

How can and holistic and integrated RM system be designed? First of all, a qualitative and quantitative analysis of the DC as well as facility service companies is required. It is necessary to examine which internal and external bases are used for the provision of services. Depending on the results, the analysis of the risk methods already implemented or yet to be implemented is carried out. The requirements can then be consolidated and combined with the criteria of the existing processes. The integration of RM into the various management systems of companies is the common denominator for identifying and controlling risks comprehensively across all service areas.

4.5 Results from expert interviews

The results of the expert discussions have shown that there is already a sufficient number of laws, norms, standards and certifications for all areas of the building LC. Table VI contains the essential core results of the expert interviews, which are interpreted as under.

Certifications		International DC companies											International FM companies											
		Apple	Amazon	Digital Realty	Equinix	Facebook	Global Switch	Google	IBM	Microsoft	Nexcenter	Telehouse	Apleona	CBRE	Caverion	Dussmann	Engie	ISS	JLL	Piepenbrock	Strabag	Spie	Sodexo	Vinci
ISO 9001	Quality	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ISO 14001	Environment			x	x		x	x	x			x	x	x	x	x	x	x		x	x	x	x	x
ISO 22301	Business Continuity Mgmt.			x	x				x	x		x												
ISO 27001	IT	x	x	x	x	x	x	x	x	x	x	x	x									x		
ISO 50001	Energy			x	x		x						x	x			x				x	x		x
ISO 55000	Asset Mgmt.																							
SOC 1,2,3	Service Organisation Control			x	x			x				x												
PCI DSS	Physical Security			x	x		x	x			x	x												
QHSAS 18001 / / ISO 45001	Health and Safety			x	x		x	x					x		x	x	x					x	x	x
Fed Ramp	Security				x			x		x														
TÜVTSI	Reliability				x			x																
Uptime	Reliability			x	x						x													
NIST 800-53/FISMA	Security			x	x																			
LEED	Environment	x		x		x	x				x													
BREEAM	Environment			x			x																	
CEEDA	Environment			x																				
ISAE 3402	IT Security						x				x													
HIPAA	Health care							x				x												
CPNI	Network											x												
SSAE16	Financial										x	x												
CSA Star	Security							x		x														
ISO 20000	IT service Mgmt.									x														
ISO 27017	Cloud security		x					x		x														
ISO 27018	Personal data		x					x		x														
DIN EN 50600	Availability Security Energy										x													
Hitrust CSF	Compliance and Risk Mgmt.							x																
GEFMA 160	Sustainability												x											
GEFMA 710	FM Excellence												x								x		x	
GEFMA 720	FM Excellence												x								x		x	
GEFMA 730	Integrated FM													x										
DIN ISO 10001	Customer satisfaction													x									x	
EG ÖKO Audit	Environment													x									x	
SCC	Safety													x	x		x						x	
ISO 77200	Security																	x		x				

Note: x = certified
Source: Own research

Table V. Certifications in data centres (own research)

Questions/indications	Experts 1	2	3	4	5	6	7	8	9	10	11
Which legislations, norms, standards, methods and certifications are known in the context of risk management in data centres?[a]	+	+	++	++	++	++	+++	++	+	++	++
RM framework known or implemented?[b]	N	Y	N	N	N	N	N	N	N	N	N
RM framework for DC industry useful?[b]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Most important aspect for RM when creating an RM framework?[c]	HF	HF	HF	SC	–	HF	–	HF	HF	HF	–

Notes: [a]None (–), few (+), some (+ +), many (+ + +), all (++++); [b]Y = Yes; N = No; [c]HF, human factor; SC, sourcing

Table VI. Results from expert interviews

The interviews with the experienced experts have shown that none of them had extensive knowledge in this area. This is due to the extreme diversity of existing fundamentals and broad scope of topic. From the experts' point of view, the common thread for a practical application of a holistic and integrated RM, which covers all areas of the LC of a DC, is missing. One of the interviewees, who works for one of the largest international DC operators, stated that an RM framework was implemented in his company. However, it turned out to be a general best practice framework that is used worldwide as a procedural standard for building operation and contains only fragmented RM components. All other experts stated that there was no holistic and integrated RM framework in the companies in which they currently operate, as well as in previous companies. There were also critical comments regarding the acceptance of this framework, as there are already many commercial institutions such as Uptime, TÜV, BICSI, etc. whose practices are internationally established. In all discussions, the human factor was most frequently mentioned as one of the largest risk factors in building operation of DC's. This reference should be considered in the context of further research and development. Based on the results of the interviews with experts from the DC market segment, there is a need to develop a special operational RM framework. From the experts' point of view, this framework can also be used in other industries with critical infrastructures. It was also suggested to identify operational RM practices in these industries and to incorporate the results into the development of the RM framework for DCs.

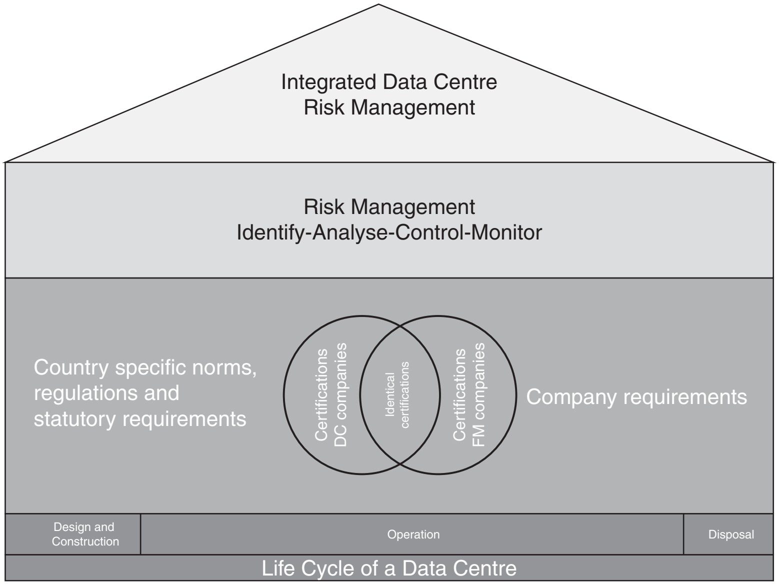
In summary, the challenge is to align the versatility of existing individual norms, standards, methodologies and certifications with practices from other industries and generate a practical application that manages risks in FM for DC more efficiently. From the perspective of the experts, the introduction of a holistic and integrated RM can help to achieve this goal and thus generate competitive advantages for DC operators.

5. Conclusions and recommendations

The research results of this paper are based on the analysis of the status and deficits of RM in FM for DC with an international perspective. This covers each of the three areas and becomes increasingly complex when combined. Literature research has shown that the diversity of existing theoretical foundations, as well as the very different interpretations of identical terms, represents the greatest challenge for a holistic and integrated RM. In addition to the large number of mandatory country-specific and cross-country legal requirements, there is a broad spectrum of optionally available norms, standards, methods and certifications. ERM is a relatively new discipline for holistic consideration in large companies and can make a fundamental contribution to eliminating the identified deficits. There are already a few research results in the scientific literature in the field of ERM that include RM frameworks such as Coso and ISO 31000:2018 (2018). However, these do not refer to the LC of DCs.

The results of the expert interviews and the analysis of applied practices support the research gaps identified in the literature and the need for an RM framework based on clear definitions and limitations. The range of theoretical foundations is so wide that even the experts lose themselves in the complexity and only have fragmented knowledge in connection with RM. Beyond the legal obligations, there is no uniformity with regard to the implementation of standards, methods and certifications. Table V illustrates how different this looks in practice. A major difficulty in this investigation was to find interview partners who were willing to provide information on the practices within the company. Even though the number of respondents was relatively small, the references to the results are clear and congruent with those from the literature search.

From the authors' point of view, a definition for an integrated RM is essential and contains the basic elements and scope described in Figure 4. This research will be continued



Note: Authors' own figure

Figure 4. Integrated risk management in data centres

on the basis of the results of this paper. The human factor as well as practices from other industries will be part of this research. The aim is to develop an RM framework for the building operation of DC considering all LC phase.

6. Limitations

The study was concluded at a macro level and did not focus on describing in detail different laws, norms, standards, certifications and RM methods as this goes beyond the scope of this paper.

Based on the results of this paper, future research shall provide more detailed analyses (qualitative and quantitative) for the implementation of a comprehensive RM system in DC. Furthermore, the interface between IT and FM functions needs to be explored taking into account the individual needs of DC companies. The investigations in this paper are limited to the LC of the building and do not relate to the IT infrastructure.

7. Notes

(1) For the purpose of confidentiality we do not name the companies used in this study here.

(2) Change management is the change life cycle process that enables beneficial changes with the minimum of disruption/risks to IT services and is described in the IT Infrastructure Library (ITIL).

(3) ERM is a holistic and company-wide risk management system.

(4) FMECA is a method which involves quantitative failure analysis to identify risks.

(5) RAMS is the abbreviation for reliability, availability, maintainability and safety and is described in DIN EN 50126-1:2017 (2017).

Notes

1. Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued Internal Control – Integrated Framework to help businesses and other entities assess and enhance their internal control systems.
2. Own and operate these facilities.
3. The term "Facility Services" relates to facility-related management services provided by (external) FM operators. Such companies are usually referred to as facility service companies.
4. IEC 31010 is currently under review and expected to be replaced by IEC/FDIS 31010 in 2020. The intension of this norm is to supplement the ISO 31000:2018 (2018) risk management standard.
5. According to Information Technology Infrastructure Library (ITIL) "Best Practice" Framework.

References

Alfen, H.W. *et al.* (2010), "Abschlussbericht zum Forschungsprojekt: Lebenszyklusorientiertes Risikomanagement für PPP-Projekte im öffentlichen Hochbau", Teill 2: Methoden des Risikomanagements, Endbericht Oktober.

Asset Insights (Ed.) (2013), *Consequences of Failure (CoF)*, available at: www.assetinsights.net/Glossary/G_Consequences_of_Failure.html (accessed 27 February 2019).

Atkin, B. and Brooks, A. (2015), *Total Facility Management*, 4th ed., Wiley, Oxford.

Atteslander, P. (2010), *Methoden der empirischen Sozialforschung*, Walter de Gruyter, Berlin.

Ben-Daya, M. *et al.* (2009), *Handbook of Maintenance Management and Engineering*, Springer, Dordrecht.

Bieser, J. and Menzel, K. (2017), "Assessing facility maintenance models for data centres: status and deficits of current facility management and maintenance concepts", *Applied Mechanics and Materials*, Vol. 887, pp. 255-263, available at: https://doi.org/10.4028/; www.scientific.net/AMM.887.255 (accessed January 2019).

Bockstefl, J. and Redlein, A. (2012), *Risikoanalyse und -bewertung für Facility Management-Prozesse während der Immobiliennnutzungsphase*, Zentrum für Informations- und Facility Management (IFM), Technische Universität Wien, Österreich.

Bromiley, P., McShane, M. and Nair, A. (2015), "Enterprise risk management: review, critique, and research directions, long range planning", *Long Range Planning*, Vol. 48 No. 4, pp. 265-276, doi: 10.1016/j.lrp.2014.07.005.

Chapelle, A. (2019), *Operational Risk Management: Best Practices in the Financial Services Industry*, Wiley, Oxford.

Cisco (Ed.) (2018), *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021*, Cisco, San Jose, CA.

Denk, R. and Exner-Merkelt, K. (2008), *Corporate Risk Management*, 2nd ed., Linde, Wien.

Dhillon, B. (2002), *Engineering Maintenance: A Modern Approach*, CRC Press, London.

Diederichs, M. (2018), *Risikomanagement und Risikocontrolling*, 4th ed., Vahlen, Munich.

EPA (1993), *Life Cycle Assessment: Inventory Guidelines and Principles*, EPA/600/R-92/245, Environmental Protection Agency, Office of Research and Development, Cincinnati, OH.

Ennouri, W. (2013), "Risks management: new literature review", *Polish Journal of Management Studies*, Vol. 8 No. 1, pp. 288-297.

GEFMA (Ed.) (2019), "Facility management", available at: www.GEFMA.de/ (accessed 15 March 2019).

Gilmore, M. (2019), "ISO 22237 vs. DIN EN 50600" (Interview) (24 March 2019).

Gleißner, W. (2016), *Grundlagen des Risikomanagements*, Vahlen, Munich.

Guicang, P. (2014), *On the Human Error in Maintenance: Risk Potential and Mitigation*, University of Stavanger-Faculty of Science and Technology, Stavanger.

Hooper, B. and O'Hare, D. (2013), *Exploring Human Error in Military Aviation Flight Safety Events Using Post-Incident Classification Systems*, ASMA, Alexandria.

Hopkin, P. (2017), *Fundamentals of Risk Management Understanding, Evaluating and Implementing Effective Risk Management*, 4th ed., IRM, London.

Huth, M., Düerkop, S. and Romeike, F. (2017), "RIMA-KIL – Risikomanagement für kritische Infrastrukturen in der Logistik", Discussion Paper No. 19, Hochschule Fulda/Fulda University of Applied Sciences Fachbereich Wirtschaft/Department of Business, Leipzig, April, available at: www.hs-fulda.de/wirtschaft.

IFMA (Ed.) (2019), *Facility Management*, IFMA, Houston, TX, available at: www.ifma.de/ (accessed 15 March 2019).

ITIL (2017), "ITIL® Glossary of Terms English v.1.0, AXELOS Limited 2011", available at: www.axelos.com/corporate/media/files/glossaries/itil_2011_glossary_gb-v1-0.pdf

Katastrophenhilfe (2018), *Bevölkerungsschutz*, Katastrophenhilfe, Bonn.

Keith, A. (1992), "Facilities management practice", *Facilities*, Vol. 10 No. 5, pp. 11-18.

Kucera, A. and Pitner, T. (2013), *Intelligent Facility Management for Sustainability and Risk Management*, Masaryk University, Faculty of Informatics Laboratory of Software Architectures and Information Systems Botanick'a 68a, 602 00 Brno, Brno.

Kunbaz, M. and Bieser, J. (2018), "An innovative approach for harmonising availability and energy efficiency in data centres: a case study", *International Review of Applied Sciences and Engineering*, Vol. 10 No. 1, pp. 93-99.

Lawrence, A. (2018), "Uptime Institute data shows outages are common, costly, and preventable", Uptime Institute Research, New York, NY, p. 10.

Levy, M. and Raviv, D. (2018), "An overview of data center metrics and a novel approach for a new family of metrics", *Advances in Science, Technology and Engineering Systems Journal*, Vol. 3 No. 2, pp. 238-251.

Marzuki, J. and Newell, G. (2019), "The emerge of data centres as an innovative alternative property sector", *Journal of Property Investment and Finance*, Vol. 37 No. 2, pp. 140-152.

Meyer, T.G.R. (2013), *Engineering Risk Management*, De Gruyter, Berlin.

O'Shea, M. and Krischanitz, C. (2013), *Comparison of the Regulatory Approach in Insurance and Banking in the Context of Solvency II*, EACG, London.

Onag, G. (2016), "Uptime Institute: 70% of DC outages due to human error", available at: www.cw.com.hk/it-hk/uptime-institute-70-dc-outages-due-to-human-error (accessed 15 March 2019).

Pakhchanyan, S. (2016), "Operational risk management in financial institutions: a literature review", *International Journal of Financial Studies*, Vol. 4 No. 4, pp. 1-21.

Ponemon Institute (Ed.) (2016), *Cost of Data Centre Outages*, Ponemon Institute, Traverse City.

Romeike, F. (2018), *Risikomanagement*, Springer Gabler, Wiesbaden.

Romeike, F. and Hager, F. (2013), *Erfolgsfaktor Risikomanagement 3.0: Lessons learned, Methoden*, Checklisten und Implementierung, 3. Aufl. Springer, Wiesbaden.

Stapelberg, R.F. (2009), *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*, Springer, London.

Tixier, J., Dusserre, G., Salvi, O. and Gaston, D. (2002), "Review of 62 risk analysis methodologies of industrial plants", *Journal of Loss Prevention in the Process Industries*, Vol. 15 No. 4, pp. 291-303, doi: 10.1016/S0950-4230(02)00008-6.

Tweeddale, M. (2003), *Managing Risk and Reliability of Process Plants*, Elsevier, Amsterdam.

Uptime (2019), "Tier standard", available at: https://uptimeinstitute.com (accessed 15 March 2019).

Wälder, K. and Wälder, O. (2017), *Methoden zur Risikomodellierung und des Risikomanagements*, Springer, Wiesbaden.

Wengert, H.S.F. (2013), *Corporate Risk Management*, Springer, Wiesbaden.

Wiggert, M. (2009), Risikomanagement von Betreiber- und Konzessionsmodellen, Graz.

Yongrok, C. *et al.* (2016), "Optimizing enterprise risk management: a literature review and critical analysis of the work of Wu and Olson", *Annals of Operations Research*, Vol. 237 No. 1, pp. 281-300.

Zheng, L. *et al.* (2016), "Overview of risk management system of commercial bank data center", *International Journal of Security and Its Applications*, Vol. 10 No. 3, pp. 245-258.

Norms, Standards, Guidelines

BS 31100, *Risk Management – Code of Practice and Guidance for the Implementation of ISO 31000*, BSI, London.

DIN 32736:2000 (2000), *Building Management – Definitions and Scope of Services*, DIN, Berlin.

DIN EN 15978:2011 (2011), *Sustainability of Construction Works – Assessment of Environmental Performance of Buildings – Calculation Method*, German version EN 15978:2011, Beuth Verlag.

DIN EN ISO/IEC 17000:2004 (2004), *Conformity Assessment – Terms and General Principles*, DIN, Berlin.

DIN EN 15221-1:2007 (2007), *Facility Management – Part 1: Terms and Definitions*, DIN, Berlin.

DIN EN 50126-1: 2017 (2017), *Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process*, DIN, Berlin.

DIN EN 50600:2016 (2016), *Information Technology – Data Centre Facilities and Infrastructures*, DIN, Berlin.

DIN EN 50600-3-1:2016 (2016), *Information Technology – Data Centre Facilities and Infrastructures – Part 3-1: Management and Operational Information*, DIN, Berlin.

GEFMA 100-1:2004 (2004), *Facility Management Grundlagen*, GEFMA, Bonn.

GEFMA 100-2:2004 (2004), *Facility Management – Leistungsspektrum*, GEFMA, Bonn.

GEFMA 192:2013 (2013), *Risikomanagement im FM – Begriffe, Methoden, Anwendungsbeispiele*, GEFMA, Bonn.

IEC 31010:2009 (2009), *Risk Management – Risk Assessment Techniques*, ISO, Geneva.

ISO 14001:2015 (2015), *Environmental Management*, ISO, Geneva.

ISO 15686-1:2011 (2011), *Building and Constructed Assets – Service Life Planning – General Principles and Framework*, ISO, Geneva.

ISO 31000:2018 (2018), *Risk Management – Guidelines*, ISO, Geneva.

ISO 41001:2017 (2017), *Facility Management – Management Systems*, ISO, Geneva.

ISO 41011:2017 (2017), *Facility management – Vocabulary*, ISO, Geneva.

ISO 41012:2017 (2017), *Facility Management – Guidance on Strategic Sourcing and The Development of Agreements*, ISO, Geneva.

ISO 41013:2017 (2017), *Facility Management – Scope, Key Concepts and Benefits*, ISO, Geneva.

ONR 49000:2014 (2014), *Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen – Umsetzung von ISO 31000 in die Praxis*, ON, Vienna.

VDI 4006:2003 (2003), *Human Reliability Methods for Quantitative Assessment of Human Reliability*, VDI, Dusseldorf.

VDI 6009:2002 (2002), *Facility-Management – Practical Basics and Application Examples*, VDI, Dusseldorf.

Further reading

EN ISO 9001:2015 (2015), *Quality Management*, ISO, Geneva.

IRM (Ed.) (2010), *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*, IRM, London.

ISO 15686-2:2012 (2012), *Building and Constructed Assets – Service Life Planning – Service Life Prediction Procedures*, ISO, Geneva.

prEN ISO 41001:2017 (2017), *Facility Management – Management Systems – Requirements with Guidance for Use*, ISO, Geneva.

Corresponding author

Juergen Bieser can be contacted at: juergen.bieser@uni-weimar.de

Appendix

Institution[a]	Life cycle category[b]	Experience of experts	RQ1[c]	RQ2[d]	RM processes/ instruments in place	Knowledge of experts
Consultancy 1 B	1	> 10 years	Each country has their own legislations that companies operate from, although there are clear ISO/DIN/BSI standards in place	An integrated RM framework would enable industry to operate from a recognised platform and develop a common understanding of the risks inherent in the DC operations. Human factor should be taken into account	Yes	1
FM Company 3 A	1,2,3,4,5	> 10 years	ISO 31000:2009 Risk Management guidelines, ISO 27002 Information security standards, Uptime Institute Tier classification system, RM framework.	Within the industry, the Tier classification systems appear to have the highest recognition. The Tier rating system is also the most specific to data centres. Human factor is most critical and has to be taken into account	Yes	1
DC Operator 1 B	1,2,3	> 25 years	H+S, working processes business risk, risk evaluation of customers; ISO standards; ISO 31000; Uptime Institute; identify-avoid-reduce-mitigate-accept, BCM, RM guidelines for critical works in combination with CMMS (Service now), risk assessments (internal+external), check lists, risk matrix for operational RM, Root cause analysis (lessons learned)	Improving present standards using examples/practices from other industries; biggest risk in the operational phase of DC belongs to a reliable maintenance and especially human factor	Yes	2
Consultancy 3 A	2,3	> 20 years	ISO 31000:2009 Risk Management guidelines, DIN EN 50600, Uptime Institute Rating and M+O Accreditation, ISO 27001, ISO 9001, ISO 14001:2015 (2015), Health and Safety legislations, SoC	Lack of ownership, to identify business risks, influence between costs and quality; RM framework integrated into supply chain	Yes	3
Consultancy 2 A	1,2	> 20 years	Uptime Institute standards, Ashrae, TIA, ANSI, BICSI, TÜV-Rheinland, many certifications to identify and eliminate	To understand the client requirements and convert them into local solutions, early involvement of specialists and integration	Yes	2

(continued)

Table AI. Expert interviews' profiles and responses with DC operators, FM companies and consultancy firms

Institution[a]	Life cycle category[b]	Experience of experts	RQ1[c]	RQ2[d]	RM processes/ instruments in place	Knowledge of experts
			risks, EN 50600, risk assessments in different kinds; Legislations: wide range of local legislations and laws for buildings, Methods: checklists, procedures to check and understand clients' requirements, software applications, e.g. BIM (design risks)	of local knowledge and key partners, RM framework should take local requirements into account (Design and Build)		
DC Operator 1 B	1,2,3,4,5	> 20 years	ISO certifications, BSI (German specific), various legislations, OEM maintenance requirements, HSEQ regulations, SOC (more US related), ISO 27001, methods: Excel-based tools, risk register (monthly reviews of all kind of risks); Certifications: different kinds	Analyses (as is situation) and collect the views from all departments, dialogue with customers to avoid colour blindness, dialogue with vendors (value retention plan), commonalities which applies for global DCs and additionally local markets /requirements, underestimation of old equipment (no spare parts, maintenance support, etc.) needs awareness of management. Human factor is biggest risk	Yes	2
DC Operator 1 B	1,2,3,4,5	> 15 years	Familiar with all of the examples quoted in "definitions" section. In addition, would include industry-specific certifications such as those from Uptime Institute focussed on Human Error (M&O, Management and Operations Certification), and on the broader context of Location Risks, Infrastructure-Related Risks and Human Error (Operational Sustainability). There are similar certifications by TÜV in Germany (expanding to other countries). Also, several of the specialised industry certifications (SOC-2, PCI, etc.) address	This is the key question. Recognising that DCs are one of the key underpinnings of our civilisation and in many cases, constitute critical infrastructures for the country or region, or even at a global level, it is necessary to have a more comprehensive, yet focussed, body of knowledge and practice for DC RM, covering: Impact of DCs in the company's (company is used here for both private as well as public companies, including government) ability to do business;	Yes	2

(*continued*)

Table AI.

Institution[a]	Life cycle category[b]	Experience of experts	RQ1[c]	RQ2[d]	RM processes/ instruments in place	Knowledge of experts
			infrastructure and operational risks in the DC, and the concept and process of RM is included in IT-specific frameworks: ITIL, ITSM, etc.	definition of "Data Centre Risk" as a result DC risks have three main aspects: Risks associated to DC failing Risks created by the DC Risks that DCs themselves are subject to during their life cycle Tools, templates, software Study of existing certifications applicable to DCs (e.g.: https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/) and generation of a DC taxonomy , so that the parts they have in common can be identified, as well as differentiating aspects. Are there certifications that, if achieved, would automatically imply that "lower level" certifications are also achieved?		
DC Operator 1 B	1,2,3,4,5	> 20 years	Telehouse certifications: ISO 9001, 27001, 3402, PCC-DSS, ISO 50001; SOC 1,2,3, Known certifications: ISO 14001:2015 (2015), Uptime Institute, ECO, TÜV; legislations: HSEQ regulations	Too many certifications in place. An integrated RM framework is useful, but it is a huge challenge against many established organisations like Uptime, TÜV, EN 50600. Human factor is the biggest risk	Yes	2
Consultancy 4 A	1	> 10 years	Methods: Excel templates, Legislations: Building and Environmental permits, Certifications.	An integrated RM framework would be a benefit for the DC industry. High investments in the DC industry needs a comprehensive RM approach. Human factor is the biggest risk.	Yes	2

(*continued*)

Table AI.

Table AI.

Institution[a]	Life cycle category[b]	Experience of experts	RQ1[c]	RQ2[d]	RM processes/ instruments in place	Knowledge of experts
DC Operator 1 B	1,2,3,4,5	> 20 years	Standards: ISO 9001, 14001, 27001, BGB, Basel 2, SAS 70, EN 50600, Methods: MoP, EOP, Change Management, RCA, Fishbone diagrams, FMECA-RAM analysis	Develop a computer model to simulate potential risk and impact, Artificial intelligent, MTTF, MTBF, construction and life cycle, CBM, Human factor with procedures in place. Human factor is the biggest risk	Yes	3
FM Company 1 B	2,3,4,5	> 15 years	Depending on projects and customers. Standards and laws are always observed. There are different standards and methods depending on application: BSI, Bitkom, Uptime, TÜV-It, DIN EN 50600, sometimes TIA 942, BICSI, PCI, SOX, ISO 27005:2008	For the management of the DC infrastructure most requirements can be covered by the current standards. However, the business of the operated IT applications is different and leads to different views. An international expanded basis/framework that deals with many topics would be sufficient	Yes	2

Notes: [a]Institution – Region: Global (1), Europe (2), the UK (3), NL (4); Revenue: > 10 Mio Euro p.a. (A), > 100 Mio Euro p.a. (B); [b]Planning (1), design (2), construction (3), operation (4), demolition (5); [c]RQ1 – How can laws, standards, methods and certifications in DCs currently applied to RM be related?; [d]RQ2 – What could serve a basis of a future holistic and integrated RM?; Knowledge of experts – basis (1), advanced (2), expert (3)
Source: Authors' expert interviews