ISAE 3402 TYP 2

Bestätigungsbericht über die Beschreibung des eingerichteten internen Kontrollsystems und die Wirksamkeit der Kontrollen

– deutsche Übersetzung des Berichts „Assurance Report on the Description of Controls, their Design and Operating Effectiveness – ISAE 3402 TYPE 2 – QSC AG – Period from January 1, 2018 to December 31, 2018" –

QSC AG
Geschäftsbereich: Infrastukturdienstleistungen
Köln

In der Zeit vom
1. Januar bis 31. Dezember 2018

KPMG AG Wirtschaftsprüfungsgesellschaft

Inhaltsverzeichnis

Anhang

Allgemeine Auftragsbedingungen

Abkürzungsverzeichnis

Abkürzung	Beschreibung
AG	Aktiengesellschaft
BCM	Betriebskontinuitätsmanagement
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCITO	SAP Services & Consulting, Cloud & IT Outsourcing
CCM	Change and Configuration Management
CERT	Computer-Notfallteam
CISO	Gesamtverantwortlicher für Informationssicherheit
CMA	Kapazitätsmanagement
CMDB	Konfigurationsverwaltungsdatenbank
CS	Central Segment
DSB	Datenschutzbeauftragter
ICMP	Internet Control Message Protocol
IP	Internet Protokoll
IPM	Incident and Problem Management
ISAE	International Standard on Assurance Engagements
ISM	Information Security Management
ISMS	Informationssicherheitsmanagementsystem
ISO	Informationssicherheitsbeauftragter
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
kV	Kilovolt
kVA	Kilovoltampere
MVA	Megavoltampere
NEA	Netzersatzanlagen
NOC	Network Operation Center
OSE	Organisatorische Sicherheit
PLS	Physical and Logical Environmental Security
RfC	Änderungsantrag
RPM	Release and Patch Management
SLA	Service-Level-Agreement
SLC	Support- and License Contract Management

TÜV	Technischer Überwachungsverein
USV	Unterbrechungsfreie Stromversorgung
VPN	Virtuelles privates Netzwerk

SECTION I

Bescheinigung über das eingerichtete Kontrollsystem und die Wirksamkeit der Kontrollen

(Erstellt durch KPMG)

Bescheinigung über das eingerichtete Kontrollsystem und die Wirksamkeit der Kontrollen (Erstellt durch KPMG)

An den Vorstand der

QSC AG, Köln,
– im Folgenden kurz „QSC" oder „Gesellschaft" –

Auftragsumfang

Wir wurden von QSC beauftragt, den Bericht sowohl über die von QSC erstellte Beschreibung der Kontrollen, dokumentiert in Abschnitt II im Zeitraum vom 1. Januar bis zum 31. Dezember 2018, als auch über den Aufbau und die Wirksamkeit der mit den in der Beschreibung vorgegebenen Kontrollzielen der Infrastukturdienstleistungen in Zusammenhang stehenden Kontrollen zu erstatten.

Der Report umfasst alle Kunden der QSC des Segments Colocation, dessen Systeme sich im Rechenzentrum von QSC in Nürnberg befinden und verwaltet werden.

Verantwortung der QSC

QSC ist verantwortlich für die Erstellung der Beschreibung und der begleitenden Erklärung in Abschnitt II (Erklärung der Dienstleistungsorganisation), einschließlich der Vollständigkeit, Richtigkeit und Methode der Darstellung der Beschreibung und der Erklärung.

QSC ist weiterhin verantwortlich für die Erbringung der von der Beschreibung erfassten Dienstleistungen, die Angabe der Kontrollziele sowie Aufbau, Implementierung und wirksame Anwendung der Kontrollen zur Erreichung der vorgegebenen Kontrollziele.

Verantwortung des Wirtschaftsprüfers KPMG

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfungshandlungen eine Beurteilung über die zutreffende Darstellung (fairness of the presentation) der von QSC beschriebenen Kontrollen als auch über die Eignung des Aufbaus (design) der Kontrollen und über die Einrichtung (implementation) sowie die Wirksamkeit (operating effectiveness) der Kontrollen zur Erreichung der in dieser Beschreibung vorgegebenen Kontrollziele abzugeben.

Wir haben unseren Auftrag unter Beachtung des vom International Auditing and Assurance Standards Board veröffentlichten International Standard on Assurance Engagements 3402, „Assurance Reports on Controls at a Service Organization (Bestätigungsbericht zu Kontrollen bei einer Dienstleistungsorganisation)", durchgeführt.

Danach sind die Prüfungshandlungen so zu planen und durchzuführen, dass mit hinreichender Sicherheit festgestellt werden kann, ob in allen wesentlichen Aspekten die Beschreibung zutreffend dargestellt, der Aufbau der Kontrollen geeignet ist und die Kontrollen eingerichtet und

wirksam sind, um die zugehörigen Kontrollziele in der Beschreibung im Zeitraum vom 1. Januar bis zum 31. Dezember 2018 zu erfüllen.

Ein Auftrag zur Berichterstattung über die Beschreibung, den Aufbau und die Effektivität der Kontrolle und bei einer Dienstleistungsorganisation beinhaltet die Durchführung von Prüfungshandlungen, um Nachweise über das durch die Dienstleistungsorganisation beschriebene System und über den Aufbau und die Einrichtung der Kontrollen zu erlangen. Die gewählten Prüfungshandlungen hängen von der Beurteilung des Dienstleistungsprüfers ab, einschließlich der Beurteilung des Risikos, dass die Beschreibung nicht zutreffend dargestellt und der Aufbau der Kontrollen nicht geeignet ist oder die Kontrollen nicht eingerichtet oder wirksam sind.

Unsere Prüfungshandlungen umfassten auch Tests der Wirksamkeit der Kontrollen, die wir als notwendig erachteten, um das Erreichen der in der Beschreibung enthaltenen Kontrollziele zu bestätigen.

Ein solcher Prüfungsauftrag umfasst auch die Bewertung der Gesamtdarstellung der Beschreibung, der Eignung der darin genannten Ziele und der Eignung der von der Serviceorganisation festgelegten Kriterien, wie in Abschnitt II dieses Berichts beschrieben.

Wir sind der Auffassung, dass die von uns erlangten Nachweise als Grundlage für unsere Beurteilung ausreichend und angemessen sind.

Unsere Unabhängigkeit und Qualitätskontrolle

Wir haben die unabhängigen ethischen Anforderungen, des vom International Ethics Standards Board for Accountants herausgegebenen Code of Ethics for Professional Accounts gefordert werden erfüllt, der auf den Grundprinzipien der Integrität, Objektivität, Fachkompetenz und Sorgfalt, Vertraulichkeit und professionelles Verhalten basiert.

Das Unternehmen wendet die International Standard on Quality Control an und unterhält dementsprechend ein umfassendes System der Qualitätskontrolle, einschließlich dokumentierter Richtlinien und Verfahren zur Einhaltung ethischer Anforderungen, beruflicher Standards und geltender gesetzlicher und regulatorischer Anforderungen.

Grenzen des Kontrollsystems bei Dienstleistungsunternehmen

Die Beschreibung der QSC ist dafür angelegt, die gemeinsamen Bedürfnisse einer großen Bandbreite von Kunden und ihrer Wirtschaftsprüfer abzudecken und kann daher nicht jeden Aspekt des Systems, das ein einzelner Kunde als wichtig für seine spezifische Umgebung erachtet, beinhalten. Ebenso, aufgrund ihrer inhärenten Eigenschaften, verhindern oder entdecken Kontrollen bei Dienstleistungsorganisationen nicht alle Fehler oder Versäumnisse bei der Bearbeitung von Transaktionen oder der Berichterstattung darüber.

Die Beschreibung der Kontrollen bei QSC erfolgt zum 31. Dezember 2018, und Informationen über Tests der operativen Wirksamkeit bestimmter Kontrollen beziehen sich auf den Zeitraum vom 1. Januar bis zum 31. Dezember 2018. Jede Projektion solcher Informationen in die Zu-

kunft birgt das Risiko, dass die Beschreibung aufgrund von Änderungen die bestehenden Kontrollen nicht mehr abbildet. Die potenzielle Wirksamkeit bestimmter Kontrollen bei QSC unterliegt inhärenten Beschränkungen, so dass potentieller Fehler oder Betrug auftreten können und nicht erkannt werden. Darüber hinaus besteht bei der Projektion von Schlussfolgerungen, die auf unseren Erkenntnissen beruhen, auf zukünftige Perioden das Risiko, dass (1) Änderungen am System oder an den Kontrollen, (2) Änderungen der Verarbeitungsanforderungen oder (3) Änderungen, die aufgrund des Zeitablaufs erforderlich sind, die Gültigkeit solcher Zusagen beeinträchtigen können.

Ergänzende Kontrollen bei den Dienstleistungsempfängern

Die Wirksamkeit spezifischer Kontrollen bei QSC und ihre Auswirkungen auf die Beurteilung des Kontrollrisikos bei Dienstleistungsempfängern hängt von ihrer Interaktion mit den Kontrollen und anderen Faktoren bei den einzelnen Dienstleistungsempfängern ab. In diesem Zusammenhang wird auf Kapitel 6 „Notwendige Kontrollen bei den Dienstleistungsempfängern" in Abschnitt II verwiesen. Wir haben keine Verfahren zur Bewertung der Wirksamkeit von Kontrollen bei einzelnen Dienstleistungsempfängern durchgeführt.

Prüfungsergebnis

Unser Urteil wurde auf der Grundlage der in diesem Bericht beschriebenen Rahmenbedingungen gebildet. Die der Bildung unseres Urteils zugrundeliegenden Kriterien sind die in Abschnitt III beschriebenen.

Nach unserer Überzeugung:

(1) stellt die dargestellte Beschreibung in allen wesentlichen Elementen die Aspekte der Kontrollen der QSC, die relevant für das interne Kontrollsystem eines Kunden bezogen auf die Prüfung der Finanzberichterstattung wie im Zeitraum vom 1. Januar bis zum 31. Dezember 2018 gestaltet und implementiert zutreffend dar;

(2) waren die beschriebenen Kontrollen in allen wesentlichen Aspekten in geeigneter Weise im Zeitraum vom 1. Januar bis zum 31. Dezember 2018 aufgebaut, um die in der Beschreibung vorgegebenen Kontrollziele zu erreichen, wenn diese Kontrollen hinreichend beachtet worden sind und die Kunden die Kontrollen, die QSC beim Design ihrer Kontrollen berücksichtigt hat, angewandt haben;

(3) getesteten Kontrollen, die wir als notwendig erachteten, um das Erreichen der in der Beschreibung enthaltenen Kontrollziele zu bestätigen, wirksam im Zeitraum vom 1. Januar bis zum 31. Dezember 2018.

Beschreibung der Prüfungshandlungen

Um unsere im vorherigen Absatz zum Ausdruck gebrachte Stellungnahme abzugeben, haben wir im Zeitraum vom 1. Januar bis zum 31. Dezember 2018 Tests an spezifischen Kontrollen,

die in Abschnitt III dieses Berichts vorgestellt werden, durchgeführt, um Bestätigung für die Wirksamkeit bei der Erreichung der in Abschnitt III beschriebenen damit verbundenen Kontrollziele zu erhalten. Die spezifischen Kontrollen sowie Art, Zeitpunkt, Umfang und Ergebnisse der Prüfungen sind in Abschnitt III aufgeführt.

Vorgesehene Berichtsempfänger und Berichtszweck

Dieser Bericht und die Beschreibung der Prüfungen und Kontrollen in Abschnitt III richtet sich nur an den Vorstand der QSC sowie an die Kunden der QSC und deren Abschlussprüfer, die über ausreichende Kenntnisse verfügen, um diesen Bericht zusammen mit weiteren Informationen, u.a. Informationen über von den Kunden selbst betriebene Kontrollen, bei der Erlangung eines Verständnisses über die für die Finanzberichterstattung relevanten Risiken der Kunden zu berücksichtigen. Der Bericht wurde nicht mit der Absicht, und darf nicht, von anderen als den hier angegebenen Parteien verwendet werden.

Zusätzliche Angaben

Wir erteilen diese Bescheinigung auf Grundlage des mit QSC AG geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die im Anhang beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften (AAB) vom 1. Januar 2017 zugrunde liegen. In Erweiterung der in Nr. 9 Abs. 2 der AAB genannten Haftungshöchstsumme von EUR 4 Mio. haftet KPMG für fahrlässig verursachte Schäden in Höhe von EUR 5 Mio. Der in Nr. 9 Abs. 5 der AAB genannte Betrag von EUR 5 Mio. bleibt unverändert. Haftungserweiterungen gelten nicht für Schäden, für die eine Haftungshöchstsumme gesetzlich geregelt ist.

Diese Haftungsbeschränkung gilt gegenüber allen Adressaten (Adressaten im Sinne dieser Regelung sind Sie selbst und alle Dritte, die unter den oben genannten Bedingungen Zugang zu unserer Berichterstattung erhalten haben), die als Gesamtgläubiger gemäß § 428 des Bürgerlichen Gesetzbuchs diese Haftung nur einmal in Anspruch nehmen können. Die Verteilung der Haftungssumme ist ausschließlich durch die Adressaten zu bestimmen; es besteht keine Verpflichtung, KPMG über den vereinbarten Gesamtgläubigerausgleich zu unterrichten. Die Gültigkeit und Höhe der Haftungsbegrenzung kann nicht mit der Begründung angefochten werden, dass eine solche Einigung unter den Adressaten nicht herbeigeführt werden konnte.

Durch Kenntnisnahme und Nutzung der in diesem Bericht enthaltenen Informationen bestätigt der Empfänger, die dort getroffenen Regelungen (einschließlich der erweiterten Haftungsregelung zu Nr. 9 Abs. 2 der Allgemeinen Auftragsbedingungen) zur Kenntnis genommen zu haben, und erkennt deren Geltung im Verhältnis zu uns an.

Hamburg, 12. März 2019

KPMG AG
Wirtschaftsprüfungsgesellschaft

Weyell
Wirtschaftsprüfer

Kramer

SECTION II

Beschreibung der Kontrollen

(Erstellt durch QSC)

1 Erklärung der Dienstleistungsorganisation

Die vorliegende Beschreibung (Section II) wurde für Kunden erstellt, die die QSC Colocation Services Anspruch genommen haben sowie für ihre Abschlussprüfer, welche ein ausreichendes Verständnis aufweisen, um diese Beschreibung bei der Bewertung des Risikos einer wesentlichen Fehlaussage des Jahresabschlusses des Kunden zusammen mit weiteren Informationen, inklusive Informationen über durch die Kunden selbst ausgeführten Kontrollen, zu berücksichtigen.

Dieser Bericht umfasst alle Systeme, die sich in dem Rechenzentrum von QSC in Nürnberg befindet und verwaltet wird.

QSC bestätigt:

(a) Die beiliegende Beschreibung in Section II stellt die System- und Prozessumgebung der Infrastrukturdienstleistungen der QSC AG und Ihrer Tochtergesellschaften im Zeitraum vom 1. Januar bis zum 31. Dezember 2018 angemessen dar. Die verwendeten Kriterien bei der Erstellung der Erklärung waren, dass die vorliegende Beschreibung:

(i) darstellt, wie die internen Kontrollen konzipiert und eingerichtet waren, inklusive:

- Der Art der erbrachten Dienstleistungen.
- Wie wesentliche Ereignisse und Bedingungen behandelt werden, abgesehen von Transaktionen.
- Relevanter Kontrollziele und konzipierter Kontrollen um diese Ziele zu erreichen.
- Kontrollen bei denen im Rahmen der Kontrollkonzeptionierung davon ausgegangen wurde, dass diese durch die Dienstleistungsempfänger implementiert wurden, können, sollte dies durch die gegebenen Kontrollziele gefordert sein, nicht durch uns alleine umgesetzt werden.
- Weitere Aspekte der Kontrollumgebung, des Risikobewertungsprozesses, der Kontrollaktivitäten, die für die Abwicklung von Kundentransaktionen relevant waren.

(ii) relevante Details über Änderungen an dem Kontrollsystem der QSC AG während des Zeitraums vom 1. Januar bis zum 31. Dezember 2018 beinhaltet;

(iii) relevante Informationen für den Anwendungsbereich der beschriebenen eingerichteten internen Kontrollen nicht auslässt oder verzerrt, wobei eingeräumt wird, dass die Beschreibung angefertigt ist, um die allgemeinen Bedürfnisse einer weiten Auswahl von Kunden und deren Abschlussprüfern zu erfüllen, und daher nicht alle Aspekte eines eingerichteten internen Kontrollsystems beinhalten kann, welche der einzelne Kunde für seine eigene spezifische Umgebung als maßgeblich erachten könnte.

(b) Die den in der vorliegenden Beschreibung ausgewiesenen Kontrollzielen zugehörigen Kontrollen waren während des Zeitraums vom 1. Januar bis zum 31. Dezember 2018 angemessen konzipiert, implementiert und wirksam. Die verwendeten Kriterien bei der Erstellung der Erklärung waren, dass

(i) die Risiken, welche die Erreichung der in der Beschreibung aufgeführten Kontrollziele gefährden, identifiziert wurden;

(ii) die identifizierten Kontrollen würden, sofern diese angewandt werden wie beschrieben, eine hinreichende Sicherheit bieten, sodass diese Risiken die Erreichung der aufgeführten Kontrollziele nicht verhindern;

(iii) die Kontrollen, inklusive der manuellen Kontrollen, wurden durchgängig wie konzipiert durch Personen, die über die entsprechende Kompetenz und Berechtigung verfügen, im Zeitraum vom 1. Januar 2018 bis 31. Dezember 2018, wie konzipiert angewendet.

(c) Fälle, in denen Probleme mit der Wirksamkeit der Kontrolle durch QSC identifiziert wurden, wurden den Wirtschaftsprüfern zur Kenntnis gebracht. Während dieses Auditzeitraums haben wir keine Abweichungen in unserem Test festgestellt.

8. Februar 2019

Stefan A. Baustert
QSC AG
Finanzvorstand

8. Februar 2019

ppa. Christoph Reif
QSC AG
Leiter Finanzen

2 Beschreibung des Unternehmens und der relevanten Bereiche

2.1 Hintergrund des Unternehmens

QSC begleitet ihre Kunden mit jahrzehntelanger Erfahrung und Kompetenz in den Bereichen Cloud, Internet of Things, Consulting und Telekommunikation sicher in das digitale Zeitalter. Mit dem Angebot von Cloud-basierten Diensten will das Unternehmen Ziele wie Geschwindigkeit, Flexibilität und Full-Service-Verfügbarkeit erreichen.

Die QSC AG beschäftigt rund 1.400 Mitarbeiter an 12 Standorten in ganz Deutschland. Die sechs TÜV und ISO zertifizierten Rechenzentren des Unternehmens in Deutschland (Frankfurt am Main, Hamburg, Köln, München, Nürnberg, Oberhausen) und das bundesweite All-IP-Netzwerk bilden die Grundlage für durchgängige Qualität und Sicherheit. Die Kunden von QSC profitieren von innovativen Produkten und Dienstleistungen aus einer Hand in den Bereichen Cloud Services & IT-Outsourcing, Internet of Things & Industry 4.0, SAP Services & Consulting, Broadband, All-IP & Network Services sowie Colocation & Virtual Datacenter.

Die QSC AG veröffentlicht als börsennotiertes Unternehmen einen jährlichen, öffentlich zugänglichen Geschäftsbericht mit weiteren aktuellen Geschäftszahlen und Fakten.

2.2 Vision und Mission

Basierend auf jahrzehntelanger Erfahrung und Expertise in den Bereichen Cloud, Consulting, Outsourcing und Telekommunikation kann die QSC AG ihre Kunden bei der Digitalisierung unterstützen. Dabei setzt die QSC AG auf bewährte, vor allem aber auf neue Technologien, viele davon sind das Ergebnis eigener Innovationen. Die QSC AG hat sich zum Ziel gesetzt Ihre Kunden als Partner zufrieden zu stellen.

Die angebotenen Dienstleistungen beziehen sich nicht nur auf Informationstechnologie, spezifische Software oder einen einzelnen Server, sondern verstehen sich als ein Prozess, der alle Bereiche eines Unternehmens bis hin zu grundlegenden Änderungen des Geschäftsmodells betrifft. Die QSC AG verfügt über das notwendige Know-how und die Erfahrung, um End-to-End Dienstleistungen zu erbringen und die Verantwortung gegenüber dem Kunden zu übernehmen.

Um ihr Know-how und ihre Compliance zu sichern und zu überprüfen, konzentriert sich die QSC AG vor allem auf die Umsetzung und Zertifizierung internationaler Normen wie ISO9001, ISO27001 und der Auditnorm ISAE3402. Während großen Anbietern oft die notwendige Agili-

tät und ein pragmatischer, unternehmerischer Ansatz fehlen, bietet QSC seinen Kunden langjährige Erfahrung, das gesamte Spektrum der IT- und Telekommunikationsdienstleistungen und die Stärken eines mittelständischen Unternehmens, zum Beispiel Agilität und Zuverlässigkeit.

2.3 Kundennutzen

QSC ist bestrebt, seinen Kunden ein Gleichgewicht zwischen Benutzerfreundlichkeit und angemessener Sicherheit zu bieten. Sie betreibt ihre gesamte Telekommunikationsinfrastruktur sowie alle ihre Rechenzentren in Deutschland und unterliegt damit den strengen gesetzlichen Anforderungen dieses Landes. Darüber hinaus verfügen unsere Mitarbeiter über langjährige Erfahrung mit Kunden, die Wert auf Sicherheit legen.

Um Geschäftsprozesse agil zu unterstützen, Kosten zu senken und Sicherheit zu gewährleisten, müssen interne IT-Umgebungen mit innovativen Anwendungen professioneller Cloud Anbieter kombiniert werden. QSC stellt dem Kunden die für diesen Zweck am besten geeignete IT-Umgebung und Plattform zur Verfügung.

Neben den traditionellen Produkten und Dienstleistungen bietet QSC auch modernste Technologien. Sie bietet ein umfassendes Portfolio in den Geschäftsbereichen Cloud, Internet of Things, Consulting, Telekommunikation und Colocation, das die wesentlichen Qualitäts-, Sicherheits- und Compliance-Anforderungen berücksichtigt und die notwendigen Maßnahmen umsetzt.

2.4 Geschäftsfelder und Lösungsportfolio

Viele der mittelständischen Kunden von QSC sind selbst Unternehmen, die anspruchsvolle Dienstleistungen anbieten, um in einem zunehmend wettbewerbsintensiven Umfeld zu bestehen. Die QSC AG überzeugt mit Kompetenz und professionellen Dienstleistungen. Dieser Anspruch erstreckt sich sowohl auf die Lösungen als auch auf die Kompetenz, das Engagement und die Denkweise der Mitarbeiter. Im Mittelpunkt des hier durchgeführten Tests stehen die implementierten Prozesse und Verfahren. QSC hat ihre Umsetzung fest in der Unternehmenskultur verankert.

Um qualitativ hochwertige Dienstleistungen anbieten zu können, ist das Lösungsportfolio von QSC in vier Geschäftsfelder unterteilt:

1. Cloud & IT Outsourcing

Im Segment Cloud & IT Outsourcing werden je nach Bedarf Outsourcing-Lösungen, Shared Services oder Cloud Services angeboten, auch in Mischformen.

Die Outsourcing-Dienstleistungen umfassen das Management von:

- von IT-Grund- und Querschnittsdienstleistungen
- geschäftskritischen Anwendungen
- stationäre und mobile Geräte
- Collaboration-Lösungen
- die Vernetzung von Unternehmensstandorten
- professionelles IT-Service-Management (ITSM)
- und einen 24/7 Service Desk als Schnittstelle zu den Mitarbeitern der Kunden.

Die Entscheidung, ob und wie die Virtualisierung erfolgen soll und ob Sicherheitsanforderungen über die Standardanforderungen hinaus gewährleistet werden sollen, wird im vertraglichen Rahmen definiert.

Für Cloud Services wurde die „Pure Enterprise Cloud" implementiert. Diese besitzt eine modulare Struktur und bietet alle wichtigen IT-Funktionen aus einer Hand und bündelt verschiedene Cloud-Welten auf einer Plattform. Der Einsatz dieser Technologie gewährleistet Flexibilität, Skalierbarkeit und Sicherheit.

2. SAP Services & Consulting

Das Segment Consulting spielt eine Schlüsselrolle bei der Digitalisierung. Dabei kommen vor allem SAP-Technologien zum Einsatz, ergänzt durch SAP HANA-Consulting und Beratung und Betrieb im Bereich des operativen Geschäfts. QSC ist ein langjähriger, zertifizierter SAP-Partner und unterstützt mit diesen Dienstleistungen über 100 Unternehmen aus den Bereichen Handel, Konsumgüter, Logistik, Energie, Anlagenbau und Maschinenbau. Die Dienstleistungen von QSC werden durch die Beratung für Microsoft Anwendungen wie SharePoint, Skype for Business und Azure ergänzt. Das Management heterogener Cloud-Umgebungen, insbesondere öffentlich-rechtlicher, privater und Multi-Cloud-Szenarien sind weitere Schwerpunkte.

3. Telekommunikation

Die Telekommunikation ist eine wichtige Säule des QSC Portfolios. Aus diesem Grund wurde dieser Bereich 2018 in eine eigene Tochtergesellschaft, die Plusnet GmbH, ausgegliedert. Die hier angebotenen Dienste basieren auf der landesweiten All-IP-Netzwerkinfrastruktur von QSC und einem leistungsfähigen Backbone. Damit verfügt QSC über ein landesweites, leistungsfähiges Netzwerk, das sich auf einen effizienten und effektiven Betrieb konzentriert. Der interne Netzbetrieb garantiert die Souveränität, Kontrolle sowie die Möglichkeit, bei Bedarf einzugreifen. Dies bedeutet, dass QSC eine gleichbleibende Qualität für die Netzwerkunterstützung seiner Cloud- und Telekommunikations Dienste bereitstellen kann.

4. Colocation

Der Schwerpunkt im Segment Colocation liegt auf dem Angebot einer sicheren und flexiblen IT-Infrastruktur. Das Unternehmen bietet Racks und Cages bis hin zu virtualisierten Lösungen an. Ergänzt wird das Leistungsportfolio durch Managementpakete und Sicherheitskonzepte. Die Services basieren auf den eigenen leistungsstarken und sicheren Rechenzentren von QSC in Deutschland, die TÜV und ISO zertifiziert sind und über eine leistungsfähige Infrastruktur miteinander verbunden sind. Links zu anderen europäischen Ländern werden in Form von mehr als 600 Peering Points angeboten.

3 Kontrollbereiche & -ziele

Kontrollbereich	Kontrollziele	Beschreibung
Organizational Security	OSE1	Das IT-Compliance Management stellt sicher, dass Organisation und Systeme im Einklang mit betrieblichen Sicherheitsleitfäden und Standards sowie den gesetzlichen und regulatorischen Erfordernissen sind.
Information Security Management	ISM1	Durch geeignete Prozesse zur Vergabe von Benutzerberechtigungen wird sichergestellt, dass sowohl Berechtigungen für Endanwender der betriebenen Systeme, als auch durch QSC AG benötigte Berechtigungen zur Administration der Systeme, durch geordnete Regel Prozessabläufe vergeben werden Diese sind Teil eines übergeordneten Sicherheits-Managements, das über Maßnahmen zur Kontrolle der ordnungsmäßigen Funktion der Prozesse zur Berechtigungsvergabe verfügt.
Change and Configuration Management	CCM1	Es ist durch ein Change Management sichergestellt, dass Änderungen an betriebenen Systemen durch Standardprozessabläufe unterstützt werden. Ein Configuration Management stellt sicher, dass Änderungen an den Konfigurationen der betriebenen Systeme sicher, abgestimmt und nachvollziehbar erfolgen
Incident and Problem Management	IPM1	Probleme und auftretende Fehler der durch die Gesellschaft betriebenen Systeme werden in unterstützenden Systemen aufgenommen, bearbeitet und verfolgt. Eine geordnete und zeitnahe Problembehebung wird durch Standardablaufprozesse sichergestellt.
Release and Patch Management	RPM1	Es bestehen Regelwerke und Arbeitsabläufe zur Durchführung von Systemaktualisierungen, wie z. B. für das Einspielen von Patches der Software- und Hardwarehersteller. Die Abläufe unterstützen sichere Aktualisierungen der betriebenen Produktionsumgebungen und berücksichtigen die Verfügbarkeitszeiten der betriebenen Systeme in angemessener Weise.

Alarm, Monitoring and Logmanagement	CMA1	Durch Überwachung der IT-Infrastruktur und eine darauf folgende Alarmierung wird sichergestellt, dass eine zeitgerechte proaktive Erkennung von Kapazitäts Engpässen oder anderen Vorfällen erfolgt. Durch geeignete Managementverfahren wird sichergestellt, dass keine Überlastung der technischen Kapazitäten erfolgt bzw. rechtzeitig Maßnahmen zur Vermeidung von Engpässen ergriffen werden können.
Support- and license contract management	SLC1	Es wird sichergestellt, dass Support- und Lizenzverträge angemessen verwaltet werden.
Business Continuity Management	BCM1	Um einen reibungslosen täglichen Systembetrieb zu gewährleisten, werden technische Überwachungssysteme und eine angemessene Prozessorganisation sowie dokumentierte Verfahren implementiert. Dadurch ist eine angemessene Reaktion auf Notfallszenarien möglich und der Systembetrieb kann nach internen Vorgaben aufrechterhalten oder wiederhergestellt werden.
Service Level Management	SLA1	Es wird sichergestellt, dass die durch vereinbarte Service Level Agreements (SLAs) gesetzten Parameter und Dienstleistungsvereinbarungen in geordneter Weise in den Regelbetrieb für die unterschiedlichen Dienstleistungen der Gesellschaft Einzug finden.
Physical and Logical Environmental Security	PLS1	Der Schutz der Hardware und Daten werden durch angemessen konzipierte und verwaltete Systeme sowie physische Einrichtungen unterstützt.

4 Änderungen der Kontrollen seit dem letzten Bericht

Um für die in Abschnitt 2.4 dargestellten vier Geschäftssegmente angemessene interne Kontrollen zu definieren und anzuwenden, wurde 2018 ein zentrales bereichsübergreifendes Kontrollsegment und geschäftsfeldspezifische Kontrollsegmente beschlossen. Aufgrund der umfangreichen Abhängigkeiten und ähnlichen Anforderungen wurden die Geschäftsfelder Consulting und Cloud & IT Outsourcing zusammengefasst. Die daraus resultierenden vier Kontrollsegmente

- Central segment (CS)
- Consulting, Cloud & IT Outsourcing (CCITO)
- Telecommunications, Plusnet (PN)
- Colocation (CL)

werden geschäftsfeldspezifisch zugeordnet und in bereichsspezifischen Berichten angezeigt. Die Kontrollen der Zentraleinheit sind für alle Geschäftssegmente anwendbar. Die daraus resultierenden relevanten Kontrollen für diesen Bericht sind die Kontrollsegmente CL und CS.

Im Vergleich zur letzten ISAE 3402-Prüfung im Jahr 2017 wurden folgende Anpassungen an den Kontrollen vorgenommen.

Segment	Kontrollen	Überarbeitete Kontroll-Referenz	Beschreibung der Änderungen
CS	OSE1-1		Eine neue Kontrolle in Bezug auf die IT-Strategie wurde eingeführt.
CS	OSE1-1	OSE1-2	Referenz geändert.
CS	OSE1-2	OSE1-3	Referenz geändert.
CS	OSE1-3	OSE1-4	Referenz geändert.
CS	OSE1-4	OSE1-5	Referenz geändert.
CS	OSE1-5	OSE1-9	Referenz geändert.
CS	OSE1-6		Eine neue Kontrolle in Bezug auf ISO 27001 und 9000 Zertifizierungen wurde eingeführt.

CS	OSE1-7		Eine neue Kontrolle in Bezug auf die Managementsysteme ISO 27001 und 9000 wurde eingeführt.
CS	OSE1-8		Es wurde eine neue Kontrolle im Bereich der Innenrevision eingeführt.
CS	OSE1-10		Eine neue Kontrolle in Bezug auf den Datenschutz wurde eingeführt.
CS	OSE1-11		Eine neue Kontrolle in Bezug auf den Datenschutz wurde eingeführt.
CS	ISM1-1		Kontrolle entfernt.
CS&CL	ISM1-2		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CS	ISM1-5		Eine neue Kontrolle in Bezug auf die Kryptographie wurde eingeführt.
CL	CMA1-2		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	IPM1-1		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	IPM1-3		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	RPM1-2 to 1-4	RPM1-1	Die Kontrollen wurden konsolidiert und die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CS	SLC1-1		Der Kontrollbereich Support- and license contract management mit der Steuerung SLC1-1 wurde in diesem Jahr eingeführt.
CL	CMA1-1		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	BCM1-1		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	BCM1-2		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	BCM1-3		Die Kontrollbeschreibung wurde angepasst, um die aktuelle Kontrollaktivität widerzuspiegeln.
CL	SLA1-1		Es wurde ein Kontrollziel bezüglich des Service Level Managements sowie eine Kontrolle hierzu eingeführt.
CL	PLS1-1		Eine neue Kontrolle in Bezug auf den physischen Zugang wurde eingeführt.
CL	PLS1-1	PLS1-2	Referenz geändert.
CL	PLS1-2	PLS1-3	Referenz geändert.
CL	PLS1-3	PLS1-4	Referenz geändert.

Darüber hinaus wurden geringfügige Änderungen in einigen Kontrollbeschreibungen (aufgrund von Formulierungs- und Tippfehlern) vorgenommen.

5 Beschreibung der Kontrollbereiche & -ziele

5.1 Organizational Security

5.1.1 Grundlagen und Abbildungen in der Organisation

Die Security Organisation der QSC AG beschäftigt sich mit Anforderungen, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Basierend auf den Anforderungen werden Prozesse, Verfahren und technische Maßnahmen festgelegt die sowohl für den Betrieb der QSC AG eigenen Systeme und Infrastruktur als auch für die angebotenen Kunden Services umgesetzt werden. Vertragliche Anforderungen seitens der Kunden die über den bei der QSC AG eigenen Grundschutz hinausgehen, führen zu einer Erhöhung der allgemeinen Standards oder aber zu entsprechenden Kunden spezifischen Ergänzungen.

Das ISMS (Informationssicherheitsmanagementsystem) der QSC AG ist orientiert sich an der vom BSI Grundschutz empfohlenen Vorgehensweise und wurde erstmals im September 2009 durch den TÜV Rheinland nach ISO 27001:2005, ab 2016 entsprechend ISO 27001:2013 zertifiziert.

Die Verantwortung für die Erfüllung der Anforderungen aus dem ISMS liegt beim Chief Information Security Officer (CISO) der QSC AG. Das zentrale Dokument ist die ISMS Leitlinie in ihr werden Strategie und Methodik des ISMS festgelegt.

Die konkrete Ausprägung und die Grundlage für die Umsetzung der Vorgaben in den einzelnen Kundenumgebungen wird durch die Rolle des Information Security Officer (ISO) verantwortet, diese Rolle wird kundenspezifisch vergeben. Die Informationssicherheitsrichtlinie enthält konkrete Sicherheitsvorgaben für die Mitarbeiter der QSC AG. Weitere Regelungen erfolgen anhand der in den ISO 27001:2013 definierten Controls, sie referenzieren aus der ISMS Dokumentation auf allgemeine Richtlinien oder aber, falls notwendig, weitere Service spezifische Regelungen. Die gesamte ISMS Dokumentation steht im Intranet allen Mitarbeitern zur Verfügung und wird im Rahmen von Audits auch den Kunden bzw. deren Auditoren zur Einsicht zur Verfügung gestellt.

Bereits in der Transitionsphase wird ein Information Security Officer (ISO) benannt. Er übernimmt später auch die Verantwortung für die Umsetzung und Überwachung der Anforderungen aus dem ISMS der QSC AG und den kundenspezifischen Anforderungen.

Rolle	Abkürzung	Zuweisung: Organisation	Erläuterung
Chief Information Security Officer	CISO	Stabsstelle Vorstand Technology & Operation	Gesamtverantwortlich für die IT- und Informationssicherheit bei der QSC AG
Information Security Officer (zum Auftraggeber)	ISO	Mitarbeiter Team ISM in der Stabsstelle CISO	Verantwortlich für IT- und Informationssicherheit bei dem Auftraggeber
Beauftragter für Informations Sicherheits Management System	ISMB	Mitarbeiter Compliance & Revision	Strategische Ausrichtung des ISMS, Definition von Anforderungen an die Informationssicherheit auf Basis der ISO 27001
Beauftragter Business Continuity Management	BCM	Mitarbeiter Compliance & Revision	Koordiniert Business Continuity- (BCM) und IT Service Continuity-Management (ITSCM) der QSC AG und der Kundenbestandteile dieser Prozesse in QSC AG Verantwortung
Datenschutzbeauftragter	DSB	Mitarbeiter Compliance & Revision mit direktem Berichtsweg zum Vorstand	Verantwortlich für alle Belange des Datenschutzes

Steuerung, Überwachung sowie Eskalationsinstanz ist der CISO, der direkt an das Management der QSC berichtet. IT- und Informationssicherheit ist aus Sicht der QSC AG integraler Bestandteil des Betriebs. Abstimmung und Kommunikationsfluss zwischen der Kundenorganisation (Service Management), dem Information Security Management (ISM) und den Fachgruppen des Betriebs werden über die Integration des Sicherheitsmanagements in zentrale Betriebsgremien sichergestellt.

Die konkrete Zuordnung der Rollen in der Ablauforganisation wird über ein monatlich aktuelles Organigramm dokumentiert.

5.1.2 Umsetzung von Vorgaben der Kunden

Im ISMS der QSC AG sind Vorgaben und Unterstützung für die Informationssicherheit in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt. Die Mitarbeiter werden mit der Informationssicherheitsleitlinie sowie der Informationssicherheitsrichtlinie der QSC AG vertraut gemacht.

Werden seitens eines Kunden ähnliche Dokumente bereitgestellt, so werden die mit den Systemen des Auftragnehmers betreuten Mitarbeiter der QSC AG ebenfalls über den gleichen Prozess auch mit den vom Kunden zur Verfügung gestellten Dokumenten unterrichtet.

5.1.3 Bereitstellung von Informationen zur Identität

Alle Personen, die sich um eine Beschäftigung bewerben, werden einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist. Im Rahmen des Identitätsmanagements bekommt jeder Person, die Zugriff auf die von der QSC AG betreuten Systeme erhält, ein personifiziertes Konto auf Basis ihrer Identität.

5.1.4 Verpflichtung des Personals

Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sind festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und über seine Unterschrift abgesichert. Sollten der Auftraggeber die bestehenden Verpflichtungserklärungen des Auftragnehmers nicht als gleichermaßen geeignet ansehen, werden die Mitarbeiter des Auftragnehmers zusätzlich gemäß der Verpflichtungserklärung des Auftragsgebers unterwiesen.

Gemäß den Regelungen für Hard- und Software der Informationssicherheitsrichtlinie darf der Anwender Systemen, die der Verwaltung der QSC AG stehen, nicht für private Zwecke nutzen. So ist der Anwender nicht befugt, die Konfiguration des Systems zu verändern.

Ebenso ist eine private Nutzung unzulässig. Hard- und Software, die nicht unter der Verwaltung der QSC IT steht, darf nicht an Systeme oder Netze der QSC AG Unternehmensgruppe angeschlossen werden. Hierzu zählt insbesondere Hard- und Software aus dem privaten Bereich sowie aus externen Quellen, d.h. von Lieferanten, Beratern, Dienstleistern oder Kunden. Private Geräte sind damit nicht für den Zugriff auf die Systeme des Auftraggebers gestattet.

5.1.5 Schulung des Personals

Im Rahmen der Sensibilisierungsmaßnahmen finden regelmäßige Online Schulungen mit wechselnden Inhalten statt. Diese bieten zum einen die Möglichkeit, sich mit dem Thema Informationssicherheit und Datenschutz tiefer zu beschäftigen und Antworten auf wichtige Fragen zu erhalten, zum anderen dienen Testfragen zur Überprüfung des eigenen Wissens. Die Einladung erfolgt per E-Mail mit einem individuellem Link. Es wird eine Schulungsquote von 80% angestrebt. Die Anwesenheit wird dokumentiert und sowohl die Trainings- als auch die Teilnahmeunterlagen können den Kunden im Rahmen von Vertragsverhandlungen zur Verfügung gestellt werden.

5.2 Information Security Management

Durch geeignete Prozesse zur Vergabe von Benutzerberechtigungen ist sichergestellt, dass durch QSC AG benötigte Berechtigungen zur Administration der Systeme durch geordnete Regelprozessabläufe vergeben werden. Diese sind Teil eines übergeordneten Sicherheits-Managements.

5.2.1 Security Incident Management

Die Definition und der Umgang mit Informationssicherheits-, Ereignissen und –Vorfällen wird über die Richtlinie Sicherheitsvorfallbehandlung beschrieben. Die notwendigen Verfahren sind implementiert und führen, soweit notwendig, durch eine enge Verzahnung mit den ITIL Prozessen (vor allem Incident- und Problem Management) zu zeitnahen Aktivitäten in den Betriebseinheiten. Dies beinhaltet die Dokumentation und Bewertung der durchgeführten Maßnahmen.

Die QSC unterscheidet dabei zwischen einem Sicherheitsereignis und einem Sicherheitsvorfall.

- Ein Sicherheitsereignis ist ein Indikator für einen Sicherheitsvorfall. Wird die Sicherheitsrelevanz erkannt oder vermutet, so wird das Ereignis in einen Incident überführt und eine initiale Security Class zugeordnet. Das passiert automatisiert oder manuell durch Setzen der Security Class für ein bestehendes Ticket bzw. der Erstellung eines Security Incidents genau für dieses Ereignis.
- Bei einem Sicherheitsvorfall hat nachweisbar ein Sicherheitsverstoß stattgefunden oder es liegen zumindest konkrete Hinweise für einen Verstoß vor.

Interne Meldewege und Eskalation von Sicherheitsvorfällen beziehen sich auf die einem Sicherheitsereignis zugeordnete Security Class (Dringlichkeit) und einer Kategorie (Schweregrad).

5.2.2 Identity- and Access Management

Prozesse für die Registrierung und Deregistrierung von Benutzern sind umgesetzt, sie berücksichtigen sowohl den Eintritt und den Wechsel als auch den Austritt eines Mitarbeiters (Joiner / Mover / Leaver Prozess). Die aus diesem Prozess oder aus der Zuweisung / Entzug einzelner Aufgaben folgende detaillierte Vergabe von Berechtigungen erfolgt soweit möglich zentral und automatisiert über das Identitymanagement der QSC AG, in jedem Fall aber dokumentiert und unter Berücksichtigung eines Freigabeverfahrens. In der Regel erfolgt eine Freigabe durch den Vorgesetzten, falls notwendig zusätzlich durch z.B. den Informationseigner.

Die Vergabe von Rechten erfolgt auf Basis eines personalisierten Accounts. Sofern die Vergabe eines personalisierten Accounts nicht möglich und das Passwort mehreren Personen zugänglich ist, wird der Zugriff auf das Passwort durch ein Passwortmanagementtool gesteuert und überwacht.

Der Aufbau und Nutzung von Passworten über eine Passwortrichtlinie definiert und wird soweit bei den jeweiligen Systemen möglich technisch durchgesetzt oder unterstützt.

Für notwendige Zugriffe von externen Umgebungen ist eine Zwei-Faktor-Authentifikation mittels eines Tokens realisiert. Für administrative Tätigkeiten werden verschlüsselte Protokolle gemäß der QSC AG Kryptographie Richtlinie verwendet.

Die Vorgaben für das Berechtigungsmanagement werden durch die Fachabteilungen in System- und Anwendungsbezogene Fachkonzepten konkretisiert und umgesetzt. Einhaltung und Umsetzung werden in regelmäßigen internen Audits überprüft.

Externe Dienstleister werden durch verbindliche Weitergabe auf die entsprechenden QSC AG Richtlinien über die Maßnahmen zu Authentifizierung und Autorisierung unterrichtet und auf ihre Einhaltung vertraglich verpflichtet.

5.2.3 Systemhardening

Die sicherere Installation, Konfiguration und Überwachung der Systeme berücksichtigt allgemeine Sicherheitsvorgaben und die Hinweise der jeweiligen Hersteller. Auf Servern dürfen Anwendungen und Softwaretools nur dann installiert und betrieben werden, wenn sie, gemäß dem Konfigurationsstandard und Betriebshandbuch, zu dem Betrieb des Servers in seiner Funktion benötigt werden.

Die Umsetzung dieser Anforderungen ist in den Servicespezifischen Konzepten und Verfahrensbeschreibungen dokumentiert und wird durch interne Audits und Security Scans überprüft.

Der Gebrauch von Programmen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und wird überwacht.

Programme und Systeme zur Erkennung von Schadsoftware und zur Vermeidung von dieser Art Software durchgeführter unerwünschter Funktionen sind verbindlich vorgeschrieben, eine Deaktivierung der Schutzfunktion ist im Normalfall nicht möglich. Notwendige Ausnahmen werden dokumentiert und in der Regel zeitlich beschränkt.

5.3 Change and Configuration Management

Das Change Management stellt sicher, dass Änderungen an den Systemen durch Standardprozesse unterstützt und entsprechend dokumentiert werden. Die Steuerung von Änderungen erfolgt bei der QSC AG über das ITSM nach ITIL im Change Management Prozess. Im Rahmen jedes Changes wird gemäß ITIL eine Risikobetrachtung durchgeführt. Bei dieser Risikobetrachtung werden auch Belange der Informationssicherheit betrachtet. Der Prozess für das Change Management ist in der Dokumentation des ITSM Managementsystems beschrieben.

Bei der QSC AG unterliegt der Einsatz von Hard- und Software einem geregelten Verfahren. Die Anforderungen dafür sind in der Verfahrensbeschreibung „Auswahl und Qualifikation von IT Assets“ dokumentiert die im Rahmen einer Ausschreibung oder von Audits eingesehen werden kann.

Auch diese Art Änderungen laufen in den Change Management Prozess, das heißt: Sind Kunden von Änderungen an Systemen unmittelbar oder mittelbar betroffen werden sie entsprechend der dort vorgesehenen allgemeinen oder auch Kunden spezifischen Verfahren informiert oder in die Entscheidung einbezogen.

Auch Wartungen werden über das Change Management geregelt, in dem der Kunden informiert wird und / oder in das Freigabeverfahren eingebunden ist.

Über die Informationssicherheitsrichtlinie der QSC AG ist der Umgang mit Daten entsprechend einer Klassifizierung generell geregelt, diese Vorgaben werden auch bei Reparatur, Wartung oder Transporten angewendet.

Jede Außerbetriebnahme wird über Line Items in der CMDB entsprechenden das Configuration Management dokumentiert. Wird im Falle von Wartung, Transport oder Außerbetriebnahme ein externer Dienstleister einbezogen, wird er vorab schriftlich auf Vertraulichkeit und Datenschutz verpflichtet.

5.4 Incident and Problem Management

Incident und Problem Management sind als zentrale ITIL Prozesse voll umfänglich dokumentiert und etabliert. Die Umsetzung der in den Prozessbeschreibungen definierten Vorgaben und die Dokumentation und Überwachung der einzelnen Vorgänge, entsprechend der mit den Kunden vereinbarten SLAs, werden durch das IT Servicemanagement System unterstützt. Dadurch ist die dokumentierte Meldung einer Störung, die Identifizierung möglicher Ursachen und die Weiterleitung an die für die Behebung der Störung zuständige Fachabteilung gesichert.

Jeder eingehende Kontakt im Service Desk erzeugt eine dokumentierte Interaktion im ITSM-System. Der Service Desk führt eine Vorqualifizierung des Incident nach Kategorisierung sowie Priorisierung und dokumentiert diese Einordnung im ITSM-Tool. Die Lösungsschritte werden im ITSM Tool dokumentiert.

Nach Behebung der Störung überprüft der Service Desk die gefundene Lösung auf Plausibilität und Verständlichkeit (z.B. gesetzte Kategorien und Beschreibung der Lösung). Nicht aussagekräftige Dokumentationen werden hierarchisch eskaliert. Ziel und Zweck ist es dem Endanwender eine klare und nachvollziehbare Dokumentation im Ticketsystem zur Verfügung zu stellen. Bei unzureichender Dokumentation wird das Ticket an die Bearbeitergruppen zurückgegeben, mit der Aufforderung zur Nachdokumentation.

Sofern eine Störung nicht nachhaltig behoben wurde oder die Störungsursache unklar ist, und damit zu rechnen ist das die Störung jederzeit wieder auftreten kann wird, bevor der Incident geschlossen wird, wird ein Problem Ticket eröffnet und unter diesem dann weiterbearbeitet.

Für kritische Vorfälle gibt es eine exakte Definition und definierte Verfahren. Die Kritikalität kann z.B. durch eine sehr große Menge an betroffenen Systemen oder Applikationen (Massenstörungen), durch Störung besonders kritischer Services der QSC AG oder ihrer Kunden oder eben auch durch kritische Sicherheitsvorfälle entstehen. Die Verfahren für kritische Vorfälle beinhalteten Eskalationsverfahren und den Einbezug besonderer Rollen und Prozesse um eine schnelle und effiziente Bearbeitung und Rückkehr in den Normalbetrieb zu ermöglichen.

5.5 Release and Patch Management

Das Ziel des Patchmanagement ist die vollständige Abdeckung aller von der QSC AG verantworteten Systeme und Applikationen mit sicherheitsrelevanten Updates. Für diese Systeme und Anwendungen wurden Fachkonzepte definiert und implementiert welche Systemspezifisch das zeitnahe und vollständige Aufbringen von Sicherheitspatchen gewährleisten. In den fachspezifischen Konzepten sind zusätzlich zu den Standard Anforderungen folgende Aspekte dokumentiert:

– Periodizität der Patchdurchläufe

– Dokumentation der Durchführung der Patchdurchläufe

Die in den Fachkonzepten festgelegten Verfahren werden als regelhaftes Patchmanagement bezeichnet.

Aufgrund der großen Bandbreite der bei unseren Kunden betriebenen Systeme und Anwendungen muss genau abgestimmt werden welche Systeme innerhalb des regelhaften Patchmanagements berücksichtigt werden. Release- und Patchmanagement von Systeme und Anwendungen außerhalb des regelhaften Patchmanagements muss explizit vertraglich vereinbart werden. Für alle nicht explizit benannten Systeme und Anwendungen liegt die Verantwortung für das Einspielen von Patches nicht bei der QSC AG. Soweit vertraglich vereinbart können Hinweise auf fehlende kundenspezifische sicherheitsrelevante Patches über das Schwachstellenmanagement erbracht werden. Der Nachweis der Patch Compliance erfolgt über das SLA Reporting. Die detaillierten Anforderungen an das Patchmanagement liegen in Form des Dokumentes „Anforderungen Patchmanagement“ vor.

5.6 Alarm, Monitoring and Logmanagement

Die automatisierte Dokumentation technischer Systeme sowie deren Überwachung und Alarmierung in Fällen von Abweichungen vom definierten Normalverhalten wird über eine ganze Reihe von Montoring- und Logmanagementwerkzeugen sichergestellt. Um in einer hochkomplexen und äusserst heterogenen IT Landschaft den Gesamtüberblick zu behalten und eine effiziente

– Überwachung der Systeme
– und Erkennung, Analyse und Bearbeitung von Vorfällen

zu ermöglichen, wurde das Unified Management Framework (UMF) definiert und etabliert. Die Informationen werden in dieser Korrelationsplattform aufbereitet und für die Betriebsgruppen in unterschiedlichen und aufgabenbezogen Sichten dargestellt und bearbeitet. Das ermöglicht eine betriebsübergeifend einheitliche und systemunabhängige Darstellung und Bearbeitung von Ereignissen. Die Ereignisse werden über die Plattform in IT Service Management Tickets überführt und im Rahmen der definierten ITIL Prozesse weiter bearbeitet.

5.7 Support and License Contract Management

Zum störungsfreien Betrieb von Systemen und Anwendungen gehört auch der Schutz der rechtzeitigen Verfügbarkeit von Herstellerinformationen und Support. Zu diesem Zweck schließt die QSC AG Support- und Lizenzverträge mit den Herstellern unter Berücksichtigung der mit den Kunden vereinbarten SLAs ab. Um einen Überblick über die oft komplexen Vertragsbeziehungen zu erhalten und eine möglichst effiziente Nutzung von Support- und Lizenzverträge zu erreichen, ist die Verantwortung für das Lizenzmanagement innerhalb der QSC AG klar definiert. Nutzungsinformationen (zeitnahe Informationen über Schwachstellen), Ansprechpartner der Hersteller, auslaufende oder zu verlängernde Verträge werden den internen Fachabteilungen und dem Kunden rechtzeitig mitgeteilt.

5.8 Business Continuity Management

5.8.1 Emergency Management

Lässt sich ein kritisches Ereignis nicht mehr im Rahmen der normalen Betriebsverfahren bearbeiten oder handelt es sich bei dem Ereignis um den Ausfall oder die Störung ganzer Betriebsbereiche oder Standorte, wird bei der QSC AG der Notfall ausgerufen und die im Business Continuity Management (BCM) definierten Verfahren kommen zur Anwendung.

Die Rahmenparameter des BCM sind in der Richtlinie zum Notfallmanagement definiert. In ihr ist die Abgrenzung zwischen Störfall, Notfall, Krise und Katastrophe definiert und es sind die für einen Notfall geltenden Rollen und Zuständigkeiten definiert. Die weiteren in der Richtlinie

definierten Anforderungen liegen in der Umsetzung in Verantwortung der einzelnen Betriebsbereiche, die Gesamtkoordination und die Prüfung der Umsetzung liegt bei dem QSC BCM Beauftragten.

Die strategische Ausrichtung und die Planungspunkte sind in dem Dokument „Notfallkonzeption und Sicherheitsstrategie der QSC AG" beschrieben. Dazu gehört auch die Beschreibung der Rahmenparameter für Notfallübungen in den einzelnen Bereichen.

Folgende Punkte sind im BCM der QSC AG definiert:

- Definitionen: Klärung wichtiger Begriffe für die allgemeingültige Bewertung sowie zielgerichtete Kommunikation und Eskalation von Ereignissen mit Schadenspotenzial für die Schutzgüter;
- Aufbauorganisation: Rollen und Verantwortlichkeiten im Rahmen des kaskadierten Notfall- und Krisenmanagements, insbesondere die im Rahmen der Krisenstabsorganisation der QSC AG wichtige lokale Krisenstabsorganisation;
- Ablauforganisation: Kommunikations- und Eskalationsprozess zur zielgerichteten und ebenengerechten Kenntnisnahme, Ereignisbewertung und bedarfsgerechten Reaktion;
- Schnittstellen und Zusammenarbeit: Darstellung der internen und externen Schnittstellen sowie der eskalationsbezogenen Kommunikationsrichtlinien;
- Technische Unterstützung: Identifikation, Festlegung und Sollforderungen für wichtige technische Hilfsmittel im Rahmen der Aufbau- und der Ablauforganisation des Notfall- und Krisenmanagements.

5.8.2 Availability Management

Für alle System- und Anwendungsdaten gibt es bei der QSC AG Unternehmensgruppe Datensicherungskonzepte. Kritische Daten, Geschäftsvorfälle und Programme werden gemäß den vertraglichen Verpflichtungen mit den Kunden gesichert. Die Vollständigkeit der geplanten Backups wird überwacht. Die auf dem persönlichen Netzlaufwerk gespeicherten Benutzerdaten werden ebenfalls gesichert. Unternehmensbezogene Daten, insbesondere sensible Daten, werden auf den entsprechenden Laufwerken der Abteilungen gespeichert.

5.9 Service Level Management

Um für die Kunden der QSC AG die vereinbarte Leistung wie vertraglich vereinbart zu liefern und diese Lieferung auch gegenüber den Kunden nachzuweisen werden mit ihnen je nach Art der Leistung und ihrem Umfang Service Level Agreements vereinbart, überwacht, gemessen und berichtet.

5.10 Physical and Logical Environmental Security

QSC AG verfügt über insgesamt 12 wesentliche Standorte in Deutschland. Für diesen ISAE 3402-Bericht wurde der Standort Nürnberg berücksichtigt.

Die physische Sicherheit variiert je nach Standort und den dort befindlichen Servicebereichen. Die Grundanforderungen werden in einer entsprechenden Richtlinie formuliert und standortspezifisch verifiziert. Grundsätzlich sind alle Standorte auf die Anforderungen der ISO27001: 2013 ausgerichtet. Das von QSC AG betriebene Datenzentrum wird in dem folgenden Unterkapitel beschrieben.

5.10.1 Rechenzentrum Nürnberg

Das Rechenzentrum erstreckt sich über vier Etagen (Keller, Erdgeschoss, erster und zweiter Stock. Zwei davon – Erdgeschoss und erster Stock – werden als RZ-Fläche genutzt).

Baujahr: 2004

Gesamtfläche: 8.000 Quadratmeter (Bruttofläche)

Notfallvorsorge: Mehrfach redundante Strom- und Klimaversorgungen sowie mehrfach redundante Kommunikationsanbindung per Glasfaser

Sicherheit: Eingefasstes, mit rund 60 Kameras videoüberwachtes Gelände und Gebäude, Personenvereinzelungsanlage, mehrstufiges elektronisches Zutrittskontrollsystem (Gebäude, Sicherheits- und Hochsicherheitsbereiche), 24/7 -Wachdienst vor Ort, Einbruchmeldeanlage

Stromversorgung: 20 KV-Netz-Versorgung

(Einspeisung in Ringtopologie), eigene Trafostation mit 20 x 1.000 kVA, 1 x 1.600 kVA, 1 x 1.250 kVA

Notstromversorgung: 13 MVA über sieben Dieselaggregate

Diesel-Vorratstank: Max. 146.000 Liter Diesel-Vorratstank

Brandschutz: Automatische Hochdruck-Inertgas-Feuerlöschanlage mit Stickstoff Löschmittel, Brandfrüherkennungs-/Rauch- und Feuermeldesysteme mit automatischer Alarmierung der Feuerwehr

Klimatechnik: Redundante Klimaschränke versorgen das Rechenzentrum, redundante Kältesysteme für die Rückkühlung, Kälteleistung insgesamt 5.8 Megawatt, überwacht durch Feuchtigkeits-, Leckage- und Wassermelder

Die Einordnung der Infrastruktur entspricht dabei folgenden TIER-Klassen:

- Entspricht grundsätzlich TIER 3+, in einigen Bereichen auch TIER 4,
- Elektroanlagen und -versorgung entspricht TIER 3+, USV entspricht TIER 4
- Kälteversorgung entspricht durchschnittlich TIER 3+,
- Brandschutz entspricht durchschnittlich TIER 3+.

Die Infrastruktur wird durch redundante Managementsysteme unterschiedlicher Hersteller kontrolliert und überwacht.

6 Notwendige Kontrollen bei den Dienstleistungsempfängern

Die Kontrollen der QSC wurden unter der Annahme entwickelt, dass spezifische Kontrollen und Verfahren von den Dienstleistungsempfängern implementiert werden. In bestimmten Situationen (siehe unterhalb) ist es notwendig, dass die Dienstleistungsempfänger spezifische Kontrollen durchführen, um bestimmte Kontrollziele zu erreichen, die in diesem Bericht spezifiziert sind.

In diesem Abschnitt werden die zusätzlichen Richtlinien, Verfahren und Kontrollen beschrieben, die in der Verantwortung der Dienstleistungsempfänger liegen, um die verwalteten Dienste und die entsprechenden Kontrollen zu ergänzen. Der unabhängige Prüfer der Dienstleistungsempfänger sollte prüfen, ob die folgenden Kontrollen bei der Benutzerorganisation in Betrieb genommen wurden.

Im Allgemeinen sind die Dienstleistungsempfänger für Prozesse oder Prozessteile verantwortlich, die nicht durch den Vertrag zwischen den Dienstleistungsempfänger und QSC abgedeckt sind.

Komplementäre Kontrollen bei Dienstleistungsempfängern für das Change und Security Management:

Information Security Management:

- Zum störungsfreien Betrieb von Systemen und Anwendungen gehört auch der Schutz der rechtzeitigen Verfügbarkeit von Herstellerinformationen und Support.
- Dienstleistungsempfänger sollten asymmetrische Schlüsselpaare oder Multifaktor-Authentifizierung verwenden, um auf ihre Hosts zuzugreifen und eine einfache passwortbasierte Authentifizierung zu vermeiden.
- Die Nutzer sind für das informieren der Behörden über Sicherheits- und Datenschutzvorfälle verantwortlich, wenn sie gesetzlich dazu verpflichtet sind.
- Die Anwendereinheiten sind für die Implementierung getrennter Entwicklungs- und Produktionskonten verantwortlich, um das Produktivsystem von der Entwicklungsarbeit zu isolieren.
- Dienstleistungsempfänger sind dafür verantwortlich, sensible Daten sowohl im Ruhezustand als auch bei der Übertragung über das Netzwerk zu verschlüsseln.

Change und Configuration Management:

- Dienstleistungsempfänger sind dafür verantwortlich, dass Personen, die Änderungsanfragen erstellen und/oder aktualisieren oder Änderungsanfragen genehmigen, über die entsprechende Berechtigung verfügen.
- Dienstleistungsempfänger sind verantwortlich für die Festlegung ihrer Geschäftsprozesse und für das Design/die Konfiguration von Anwendungen und Konfigurationskontrollen, die zur Unterstützung des Geschäftsprozesses erforderlich sind.
- Dienstleistungsempfänger sind für die Zuweisung geeigneter Ressourcen zur Definition und zum Testen ihrer Systeme verantwortlich. Die Prüfung sollte Verfahren umfassen, die notwendig sind, um die Funktionalität des Systems zu ermitteln und um festzustellen, ob die Systemkontrollen korrekt konfiguriert wurden.

Release und Patch Management:

- Dienstleistungsempfänger sind dafür verantwortlich, die notwendigen Patches zu autorisieren.

Service Level Management:

- Dienstleistungsempfänger sind dafür verantwortlich, die Erbringung der von QSC erbrachten Dienstleistungen zu überwachen.

Die oben beschriebenen Überlegungen im Hinblick auf die Anwenderkontrollen erheben keinen Anspruch auf Vollständigkeit. Bei den Dienstleistungsempfängern können weitere Kontrollen erforderlich sein.

SECTION III

Kontrollziele, verbundene Kontrollen und Prüfung der Wirksamkeit der Kontrollen für QSC AG

(Erstellt durch KPMG)

7 Ziele und Durchführung der Prüfung

Dieser Bericht über die eingeführten Kontrollen und deren Wirksamkeitsprüfungen soll interessierten Parteien ausreichende Information liefern, um ein Verständnis für die Aspekte des von der QSC AG aufgesetzten Kontrollsystems zu ermöglichen, die Relevanz für das interne Kontrollsystem der Kunden der QSC AG besitzen.

Die interessierten Parteien sind definiert als das Management der QSC AG, deren Kunden und den unabhängigen Wirtschaftsprüfern der Kunden. Die Kontrollbeschreibungen, die in diesem Report definiert sind, repräsentieren alle materiellen Aspekte der relevanten Kontrollstrukturen der QSC. Ebenso, kombiniert mit dem Verständnis bezogen auf das interne Kontrollsystem der Kundenorganisationen, soll der Report bei der Bewertung aller implementierten Kontrollen im Zusammenhang mit den durch die QSC verarbeiteten Transaktionen helfen.

Die Prüfung der KPMG beschränkte sich auf Kontrollen im Zusammenhang mit folgenden Prozessen:

- Organizational Security
- Information Security Management
- Change and Configuration Management
- Incident and Problem Management
- Release and Patch Management
- Alarm, Monitoring and Log Management
- Support and License Contract Management
- Business Continuity Management
- Service Level Management
- Physical and Logical Environmental Security

Die Prüfungsaktivitäten beschränkten sich auf Prozesse, die den Kundenorganisationen der QSC AG zur Verfügung gestellt wurden und erstreckten sich dementsprechend nicht auf die Prozesse, die bei den Kundenorganisationen vorhanden sind. Unsere Prüfung wurde in Übereinstimmung mit dem Internationalen Standard für die Prüfung von internen Kontrollsystemen 3402, „Assurance Reports on Controls at a Service Organization", herausgegeben vom International Auditing and Assurance Standards Board, durchgeführt.

Es liegt in der Verantwortung jedes Beteiligten, diese Informationen in Bezug auf die internen Kontrollen der Kundenorganisation zu bewerten, um ein Verständnis der Kontrollen zu erlangen und das Kontrollrisiko zu bewerten. Die Steuerelemente der Kundenorganisationen und

der QSC AG müssen zusammen ausgewertet werden. Wenn wirksame Kontrollen bei Benutzerorganisationen nicht vorhanden sind, können die QSC-Kontrollen solche Schwächen nicht ausgleichen.

Die Beschreibung der Kontrollziele unterliegt der Verantwortung des QSC-Managements. KPMG hat die Aufgabe, zu beurteilen, ob die Kontrollen mit hinreichender Wirksamkeit betrieben werden, um eine angemessene, jedoch nicht absolute Sicherheit zu gewährleisten, dass die vom QSC-Management festgelegten Kontrollziele im Berichtszeitraum erreicht wurden.

Unsere Kontrolltests erstrecken sich auf den Zeitraum vom 1. Januar bis 31. Dezember 2018 und wurden auf die Kontrollen in Verbindung mit den durch QSC definierten Kontrollzielen angewendet.

8 Beschreibung durchgeführter Prüfungshandlungen

Unsere Prüfungshandlungen zur Wirksamkeit der Kontrollen umfassten die folgenden Aktivitäten:

Typ	Beschreibung
Befragung	Gespräche mit den zuständigen Mitarbeitern zur zeitlichen Durchführung von Kontrollen, der Ergebnisse von Kontrollmaßnahmen und der Dokumentation von Kontrollen.
Walkthrough	Erläuterung und Demonstration von bereitgestellten Prozessbeschreibungen oder zusätzlicher Dokumentation (einschließlich der Kontrollaktivitäten) durch die mit der Durchführung betrauten Mitarbeiter.
Einsichtnahme	Durchsicht von Dokumentationen und Berichten, die einen Einblick in die Arbeitsabläufe und die Durchführung von Kontrollen geben. Dies beinhaltete unter anderem: – Durchsicht von Organisationsanweisungen – Einsichtnahme in Kontrolldokumentation – Einsichtnahme in Auswertungen zu Kontrolldurchführungen
Beobachtung	Beobachtung der Durchführung spezifischer Kontrollhandlungen.
Re-Performance	Erneute Durchführung ausgewählter Transaktionen oder Kontrollen, die in entsprechender Prozessbeschreibung oder Dokumentation beschrieben sind.

9 Prüfung der Service Organization Assertion

Wir haben die folgenden Prüfungshandlungen im Zusammenhang mit der Service Organization Assertion (vgl. Section II, Kapitel 1) durchgeführt:

Einsichtnahme in die durch die QSC AG bereitgestellte schriftliche Version der Service Organization Assertion. Befragung des QSC Managements, Herrn Martin Kraus (Head Internal Audit and Compliance), hinsichtlich der Details der Service Organization Assertion:

- Inhalt und Verantwortlichkeiten des geprüften internen Kontrollsystems
- Wiederkehrende Aktivitäten zur Sicherstellung der Einhaltung definierter Berichtswege sowie der Verfolgung festgestellter Abweichungen im Rahmen der Prüfungsaktivitäten

Auf Grundlage unserer dargestellten Prüfungshandlungen wurden keine Abweichungen hinsichtlich der Service Organization Assertion festgestellt.

10 Darstellung der durchgeführten Prüfungshandlungen einschließlich der Kontrollziele und geprüften Kontrollen

10.1 Organizational Security

Kontrollbereich				
OSE1 – Das IT-Compliance Management stellt sicher, dass Organisation und Systeme im Einklang mit betrieblichen Sicherheitsleitfäden und Standards sowie den gesetzlichen und regulatorischen Erfordernissen sind.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
OSE1-1	CS	Das Unternehmen hat eine IT-Strategie definiert, die mit der Geschäftsstrategie übereinstimmt. Diese Strategie definiert strategische Ziele für den Einsatz der IT sowie Anforderungen an die Gestaltung von IT-Systemen und Anwendungen.	Befragung der Prozessverantwortlichen zur IT-Strategie.	Keine Beanstandungen
			Überprüfung des aktuellsten IT-Strategiedokuments und Überprüfung, ob strategische Ziele definiert sind.	
OSE1-2	CS	Die Gesellschaft verfügt über eine schriftlich dokumentierte Organisationsstruktur über welche Aufgabenfelder definiert werden, die den Mitarbeitern bekannt sind. Die Organisationsstruktur unterstützt eine überschneidungsfreie Definition von Rollen und Verantwortlichkeiten innerhalb der Gesellschaft.	Prüfung der Organisationsstruktur im Hinblick auf definierte funktionale Aufgabentrennung und zeitnaher Fortschreibungsprozess des Dokuments.	Keine Beanstandungen
			Überprüfung der Veröffentlichung des Dokuments.	

Kontrollbereich				
OSE1 – Das IT-Compliance Management stellt sicher, dass Organisation und Systeme im Einklang mit betrieblichen Sicherheitsleitfäden und Standards sowie den gesetzlichen und regulatorischen Erfordernissen sind.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
OSE1-3	CS	Die IT-Sicherheitsrichtlinie ist in schriftlicher Form verständlich dokumentiert und wird regelmäßig aktualisiert. Sie ist von zuständiger Managementebene freigegeben. Die Sicherheitsrichtlinie ist für jeden Mitarbeiter frei zugänglich und somit in der Gesellschaft kommuniziert.	Prüfung der Informationssicherheitsrichtlinie auf Aktualität und Vollständigkeit. Überprüfung der Verfügbarkeit der Dokumente im Intranet des Unternehmens und ermittelt, dass es kürzlich aktualisiert, überprüft und genehmigt wurde.	Keine Beanstandungen
OSE1-4	CS	Prozesse des Personalwesens stellen sicher, dass für Aufgaben und Dienstleistungen angemessen qualifiziertes Personal eingestellt wird, Verpflichtungserklärungen gemäß den Datenschutzgesetzen unterschrieben werden und soweit erforderlich Mitarbeiter vor der Einstellung einer Sicherheitsüberprüfung unterzogen werden.	Überprüfung des Prozessdesigns und der verwendeten Vorlagen.	Keine Beanstandungen
OSE1-5	CS	Für relevante Sicherheitsbereiche wurden entsprechende Rollen etabliert, die adäquat in die Unternehmensorganisation eingebunden sind. Diese beinhalten die Rolle eines Informationssicherheitsbeauftragten, eines BCM Beauftragten sowie eines Datenschutzbeauftragten.	Einsichtnahme in den Prozess zur Berufung des Informationssicherheitsbeauftragten und Datenschutzbeauftragten bezüglich der Definition von Verantwortlichkeiten und sicherheitsrelevanten Aufgabenbereichen. Prüfung der formellen Dokumente bezüglich der offiziellen Bekanntgabe der oben genannten Positionen.	Keine Beanstandungen

Kontrollbereich				
OSE1 – Das IT-Compliance Management stellt sicher, dass Organisation und Systeme im Einklang mit betrieblichen Sicherheitsleitfäden und Standards sowie den gesetzlichen und regulatorischen Erfordernissen sind.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
OSE1-6	CS	Implementierte Managementsysteme wurden nach ISO27001 und ISO9000 zertifiziert. Entsprechend gültige Zertifikate liegen vor.	Befragung von Prozessverantwortlichen zur Zertifizierung von Managementsystemen. Prüfung ob die ISO-Zertifizierungen und deren Validität für die Prüfungsperiode.	Keine Beanstandungen
OSE1-7	CS	Interne Audits für die etablierten Managementsysteme (Informationssicherheit, Datenschutz, Qualitätsmanagement) werden regelmäßig durchgeführt.	Befragung des verantwortlichen Personals hinsichtlich der Durchführung von internen Audits während des Auditzeitraums. Überprüfung der internen Auditberichte auf Stichprobenbasis.	Keine Beanstandungen
OSE1-8	CS	Die Ergebnisse der internen Audits werden bewertet und notwendige Maßnahmen abgeleitet.	Befragung des verantwortlichen Personals hinsichtlich der Risikoanalyse und der abgeleiteten Maßnahmen. Einsichtnahme in die Berichte der internen Audits hinsichtlich der durchgeführten Risikoanalysen und der daraus abgeleiteten Maßnahmen.	Keine Beanstandungen
OSE1-9	CS	Im Sinne eines fortlaufenden Prozesses werden die Maßnahmen zur Risikominimierung unter Verantwortung der Unternehmensleitung durch einen Risikomanager geprüft. Es werden neben allen relevanten Assets die Gewichtung der Bedrohungen und die Einstufung in Risikoklassen in Bezug auf das IT-Szenario der QSC AG betrachtet. Die Risikoeinstufung wird mindestens jährlich geprüft und gegebenenfalls angepasst.	Einsichtnahme in die Richtlinie zum Umgang mit Risiken bei der QSC AG und ihren verbundenen Unternehmen. Plausibilisierung des eingesetzten Risiko Managementverfahrens mit dem Risikomanager. Prüfung des Dokumentes auf Aktualität der definierten Risiken und Risikokategorien. Stichprobenhafte Prüfung der durchgeführten Risikountersuchungen der Gesellschaft.	Keine Beanstandungen

Kontrollbereich				
OSE1 – Das IT-Compliance Management stellt sicher, dass Organisation und Systeme im Einklang mit betrieblichen Sicherheitsleitfäden und Standards sowie den gesetzlichen und regulatorischen Erfordernissen sind.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
OSE1-10	CS	Regulatorische Anforderungen an den Datenschutz sind in der Datenschutzrichtlinie berücksichtigt. Datenschutzschulungen der Mitarbeiter werden regelmäßig durchgeführt.	Befragung des Datenschutzbeauftragten zur Umsetzung der Datenschutzanforderungen einschließlich Datenschutzkurse. Überprüfung der Datenschutzerklärung und Überprüfung, ob wesentliche Datenschutzelemente berücksichtigt werden. Stichprobenartig überprüft, dass die im Jahr 2018 eingestellten Mitarbeiter die Datenschutzschulung absolviert haben.	Keine Beanstandungen
OSE1-11a	CS	Das Verarbeitungsverzeichnis wird regelmäßig aktualisiert und umfasst alle wesentlichen Bereiche der QSC AG. Technische und organisatorischen Maßnahmen (TOM) sind definiert und implementiert.	Befragung des Datenschutzbeauftragten bezüglich der Führung des Verarbeitungsverzeichnisses und der getroffenen technischen und organisatorischen Maßnahmen. Überprüfung des Verarbeitungsverzeichnisses und Überprüfung, ob die wesentlichen Verarbeitungen dokumentiert sind und ob das Verzeichnis regelmäßig aktualisiert wurde. Überprüfung der Listen, die identifizierte Anwendungen und Prozesse dokumentieren.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrollen ausreichend wirksam sowie geeignet sind, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.2 Information Security Management

Kontrollbeschreibung
ISM1 – Durch geeignete Prozesse zur Vergabe von Benutzerberechtigungen wird sichergestellt, dass sowohl Berechtigungen für Endanwender der betriebenen Systeme, als auch durch QSC AG benötigte Berechtigungen zur Administration der Systeme, durch geordnete Regel Prozessabläufe vergeben werden Diese sind Teil eines übergeordneten Sicherheits-Managements, das über Maßnahmen zur Kontrolle der ordnungsmäßigen Funktion der Prozesse zur Berechtigungsvergabe verfügt.

Kontroll ID	Segment	Kontrollbeschreibung von QSC	Prüfungshandlungen von KPMG	Prüfungsergebnis
ISM1-2	CS&CL	Der Zugang zu kritischen Systemen ist über Berechtigungskonzepte und nach Funktionstrennungsgesichtspunkten eingeschränkt. Es wird sichergestellt, dass nur autorisierte und notwendige Personen weitreichende Berechtigungen (Administratorenkennungen) für Betriebssysteme und Datenbanken haben.	Interview mit dem Verantwortlichen bezüglich des Superuserzugriffs auf Betriebssysteme und Datenbanken.	Keine Beanstandungen
			Prüfung der Berechtigungskonzepte unter funktionalen Trennungsaspekten Prüfung von des Superuser-Accounts auf Linux-, Windows- und Datenbanksystemen und Prüfung der Angemessenheit der Vergabe von Superuserrechten.	
ISM1-3	CL	Ein angemessenes Benutzermanagement ist zur Berechtigungsadministration für Server Betriebssysteme ist eingerichtet. Dieses umfasst eine geordnete Berechtigungsvergabe, -änderung und -löschung.	Überprüfung des Vorhandenseins von Berechtigungskonzepten, die den Zugriff auf Server-Betriebssysteme beschreiben sowie die Zuordnung von Berechtigungen und das Löschen von Berechtigungen.	Keine Beanstandungen
			Prüfung der Zuweisung, Änderung und Löschung von Berechtigungen. Darüber hinaus haben wir in einer Stichprobe geprüft, dass der VPN-Zugang ehemaliger Mitarbeiter zeitnah gesperrt/deaktiviert wurde.	

Kontrollbeschreibung				
ISM1 – Durch geeignete Prozesse zur Vergabe von Benutzerberechtigungen wird sichergestellt, dass sowohl Berechtigungen für Endanwender der betriebenen Systeme, als auch durch QSC AG benötigte Berechtigungen zur Administration der Systeme, durch geordnete Regel Prozessabläufe vergeben werden Diese sind Teil eines übergeordneten Sicherheits-Managements, das über Maßnahmen zur Kontrolle der ordnungsmäßigen Funktion der Prozesse zur Berechtigungsvergabe verfügt.				
Kontroll ID	**Segment**	**Kontrollbeschreibung von QSC**	**Prüfungshandlungen von KPMG**	**Prüfungsergebnis**
ISM1-5	CS	Angemessene Verschlüsselungstechnologien und Verfahren sind in einer Kryptographie Richtlinie berücksichtigt. Diese Richtlinie regelt unter anderem die Verschlüsselung vertraulicher Informationen und Kommunikationswege sowie das Schlüsselmanagement.	Abfrage des Prozesseigners nach der Kryptographie Richtlinie. Überprüfung der Kryptographie Richtlinie unter Berücksichtigung aktueller Standards wie z.B. Verschlüsselungsalgorithmen.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrollen ausreichend wirksam sowie geeignet sind, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.3 Change and Configuration Management

Kontrollbeschreibung
CCM1 – Es ist durch ein Change Management sichergestellt, dass Änderungen an betriebenen Systemen durch Standardprozessabläufe unterstützt werden. Ein Configuration Management stellt sicher, dass Änderungen an den Konfigurationen der betriebenen Systeme sicher, abgestimmt und nachvollziehbar erfolgen.

Kontroll ID	Segment	Kontrollbeschreibung	Prüfungshandlungen	Prüfungsergebnis
CCM1-1	CL	Change Management Prozesse für eine angemessene Bearbeitung von Änderungen sind implementiert und dokumentiert. Die Bearbeitung der Änderungen wird durch geeignete Softwareprogramme unterstützt.	Interview mit dem Prozessverantwortlichen und Einsichtnahme in die Dokumente zum Change Management. Prüfung, ob das ITSM-System zum Verwalten von Änderungen verwendet wurde. Prüfung ob die Prozessdokumentation zum Change Management im Intranet verfügbar ist.	Keine Beanstandungen
CCM1-2	CL	Änderungen im Rahmen des Change Managements werden zeitnah und anforderungsgemäß durchgeführt.	Prüfung der implementierten Change Management Prozesse im Hinblick auf die anforderungsgerechte Implementierung.	Keine Beanstandungen

Kontrollbeschreibung				
CCM1 – Es ist durch ein Change Management sichergestellt, dass Änderungen an betriebenen Systemen durch Standardprozessabläufe unterstützt werden. Ein Configuration Management stellt sicher, dass Änderungen an den Konfigurationen der betriebenen Systeme sicher, abgestimmt und nachvollziehbar erfolgen.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
CCM1-3	CL	Configuration Management Prozesse, die eine angemessene Pflege der Konfiguration unterstützen, sind implementiert. Konfigurationen im Rahmen des Configuration Managements sind gepflegt und dessen Bearbeitung wird durch geeignete Softwareprogramme unterstützt.	Befragung der Prozessverantwortlichen zum Configuration Management. Inspektion des Systems, das zur Pflege von Konfigurationen verwendet wird. Stichprobenartige Prüfung, dass Konfigurationen in der Management-Datenbank dokumentiert sind.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrollen ausreichend wirksam sowie geeignet sind, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.4 Incident and Problem Management

Kontrollbeschreibung				
IPM1 – Probleme und auftretende Fehler der durch die Gesellschaft betriebenen Systeme werden in unterstützenden Systemen aufgenommen, bearbeitet und verfolgt. Eine geordnete und zeitnahe Problembehebung wird durch Standardablaufprozesse sichergestellt.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
IPM1-1	CL	Incident und Problem Management Prozesse für eine angemessene Bearbeitung von Fehlern sowie Problemen sind implementiert. Die Bearbeitung wird durch geeignete Softwareprogramme unterstützt. Die Verfahren sind in allen Geschäftsbereichen etabliert. Neben einer zentralen Sicht existieren Auswertungsmöglichkeiten nach Geschäftsbereichen und Mandanten.	Gespräch mit dem Prozessverantwortlichen und Einsichtnahme in die Dokumente zum Incident- und Problem Management sowie Prüfung ob der Prozess gängigen Incident und Problem Management Methoden entspricht. Einsichtnahme in das zur Durchführung von Incident und Problem Management Prozessen verwendeten Softwareprogramm und Überprüfung, dass eine Auswertung nach Geschäftsbereichen und Kunden möglich ist.	Keine Beanstandungen
IPM1-2	CL	Stör- und Ausfälle werden, sofern vertraglich vereinbart, gemeldet und entsprechend der Richtlinien behandelt. Ein 1st Level Support als Single-Point-of-Contact ist eingerichtet. Eine zeitnahe und geordnete Behebung der Störungen wird in Übereinstimmung mit dem definierten Incident und Problem Management Prozess durchgeführt.	Überprüfen Sie die vertraglichen Verpflichtungen und definierten Prozesse. Prüfung von Incident Tickets in Stichproben und Prüfung, ob die Incidents angemessen dokumentiert und zeitnah bearbeitet wurden. Darüber hinaus haben wir geprüft, ob ein 1st Level Support implementiert ist.	Keine Beanstandungen

Kontrollbeschreibung				
IPM1 – Probleme und auftretende Fehler der durch die Gesellschaft betriebenen Systeme werden in unterstützenden Systemen aufgenommen, bearbeitet und verfolgt. Eine geordnete und zeitnahe Problembehebung wird durch Standardablaufprozesse sichergestellt.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
IPM1-3	CL	Kritische Störfälle werden nach einem gesonderten Verfahren (Major Incident Prozess) eskaliert und bearbeitet. Sie werden an die zuständigen internen und soweit gesetzlich vorgegeben oder bei expliziter vertraglicher Vereinbarungen an externe Stellen gemeldet.	Befragung des Prozessverantwortlichen bezüglich des Major Incident Prozesses. Prüfung der Tickets von Major Incident in Stichproben und Prüfung, ob die Vorfälle ordnungsgemäß klassifiziert und ordnungsgemäß dokumentiert, verarbeitet und zeitnah gemeldet wurden.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrollen ausreichend wirksam sowie geeignet sind, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.5 Release and Patch Management

Kontrollbeschreibung				
RPM1 – Es bestehen Regelwerke und Arbeitsabläufe zur Durchführung von Systemaktualisierungen, wie z. B. für das Einspielen von Patches der Software- und Hardwarehersteller. Die Abläufe unterstützen sichere Aktualisierungen der betriebenen Produktionsumgebungen.				
Kontroll ID	**Location**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
RPM1-1	CL	Es bestehen Regelwerke und Arbeitsabläufe zur Durchführung von Systemaktualisierungen, wie bspw. für das Einspielen von Patches der Software- und Hardwarehersteller.	Prüfung des Release und Patch Management-Prozesses. Interview mit den Prozessverantwortlichen und Prüfung der Patch Management-Dokumentation. Prüfung der durchgeführten Patche und Release auf Stichprobenbasis und Überprüfung, ob die Releases angemessen dokumentiert wurden.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrolle ausreichend wirksam sowie geeignet ist, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.6 Alarm, Monitoring and Logmanagement

Kontrollbeschreibung
CMA1 – Durch Überwachung der IT-Infrastruktur und eine darauf folgende Alarmierung wird sichergestellt, dass eine zeit-gerechte proaktive Erkennung von Kapazitäts Engpässen oder anderen Vorfällen erfolgt. Durch geeignete Managementverfahren wird sichergestellt, dass keine Überlastung der technischen Kapazitäten erfolgt bzw. rechtzeitig Maßnahmen zur Vermeidung von Engpässen ergriffen werden können.

Kontroll ID	Segment	Kontrollbeschreibung	Prüfungshandlungen	Prüfungsergebnis
CMA1-1	CL	Es sind Prozesse und Verfahren zur Systemüberwachung und Erkennung von Überlastungen technischer Ressourcen eingerichtet.	Prüfung der Maßnahmen zur Überwachung der technischen Ressourcen durch Monitoring-Verfahren. Prüfung von Maßnahmen zur Überwachung der technischen Ressourcen. Einsichtnahme in die Dokumentation der durchgeführten Überwachungsmaßnahmen.	Keine Beanstandungen

Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrolle ausreichend wirksam sowie geeignet ist, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.

10.7 Support and License Contract Management

Kontrollbeschreibung				
SLC1 – Es wird sichergestellt, dass Support- und Lizenzverträge angemessen verwaltet werden.				
Kontroll ID	**Segment**	**Kontrollbeschreibung von QSC**	**Prüfungshandlungen**	**Prüfungsergebnis**
SLC1-1	CS	Support- und Lizenzvertragsinformationen werden zentral gespeichert. Es wird sichergestellt, dass die Fristen für die Verträge dokumentiert werden und die Verantwortlichen vor Ablauf des Vertrages erinnert werden. Die Verantwortlichkeiten für Support- und Lizenzverträge sind klar definiert.	Befragung der Prozessverantwortlichen bezüglich des Managements von Support- und Lizenzverträgen und der automatisierten Prüfverfahren. Überprüfung der Vertragsdirektion und Überprüfung der Konfiguration hinsichtlich der automatisierten Verlängerungserinnerungen. Darüber hinaus haben wir festgestellt, dass Mitteilungen über die Verwendung von Pfandkrediten erstellt wurden und das die Verantwortlichkeiten für Support- und Lizenzverträge sind klar definiert sind.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrolle ausreichend wirksam sowie geeignet ist, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.8 Business Continuity Management

Kontrollbeschreibung				
BCM1 – Um einen reibungslosen täglichen Systembetrieb zu gewährleisten, werden technische Überwachungssysteme und eine angemessene Prozessorganisation sowie dokumentierte Verfahren implementiert. Dadurch ist eine angemessene Reaktion auf Notfallszenarien möglich und der Systembetrieb kann nach internen Vorgaben aufrechterhalten oder wiederhergestellt werden.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
BCM1-1	CS	Das Notfall-, Krisen- und Katastrophenmanagement ist definiert und in schriftlicher Form verständlich dokumentiert. Die Dokumentation wird regelmäßig aktualisiert und ist von zuständiger Managementebene freigegeben. Die Dokumentation ist für jeden Mitarbeiter frei zugänglich und im Unternehmen kommuniziert.	Befragung der Prozessverantwortlichen zum Notfallkonzept im Hinblick auf diese Gültigkeit und Genehmigung durch das Management. Prüfung des Notfallkonzeptes hinsichtlich der Inhalte, Managementfreigabe und der Verfügbarkeit der Dokumente im Intranet des QSC.	Keine Beanstandungen
BCM1-2	CS	Für den Umgang mit Notfällen, Krisen und Katastrophen sind die dafür notwendigen Prozesse, Verfahren und eine Organisation beschrieben. Maßnahmen sind für verschiedene Szenarien dokumentiert und Kontaktdaten verantwortlicher Personen nach Funktion und Zuständigkeitsbereich aufgeführt. Der Umgang mit den definierten Notfallsituationen wird abgedeckt durch Wartungsarbeiten, Änderungen, Stör- und Ausfälle sowie insbesondere den kritischen Störfällen.	Befragung der Prozessverantwortlichen zu den konsolidierten Szenarien und den dokumentierten Instandhaltungsarbeiten. Prüfung, ob konsolidierte Szenarien definiert und verantwortliche Rollen dokumentiert werden. Darüber hinaus haben wir untersucht, dass Notfallsituationen im Rahmen von Instandhaltungsarbeiten, Änderungen, Vorfällen und Großereignissen abgedeckt werden.	Keine Beanstandungen

Kontrollbeschreibung				
BCM1 – Um einen reibungslosen täglichen Systembetrieb zu gewährleisten, werden technische Überwachungssysteme und eine angemessene Prozessorganisation sowie dokumentierte Verfahren implementiert. Dadurch ist eine angemessene Reaktion auf Notfallszenarien möglich und der Systembetrieb kann nach internen Vorgaben aufrechterhalten oder wiederhergestellt werden.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
BCM1-3	CL	Kritische Daten, Geschäftsvorfälle und Programme werden gemäß den vertraglichen Verpflichtungen mit den Kunden gesichert. Die Vollständigkeit der geplanten Backups wird überwacht. Die Verfahren sind in allen Geschäftsbereichen etabliert. Neben einer zentralen Sicht gibt es Auswertungsmöglichkeiten nach Geschäftsbereichen und Mandanten.	Befragung der Prozessverantwortlichen bezüglich der Durchführung und Überwachung der Backups. Überprüfung des implementierten Prozesses zur Statusüberwachung von Datensicherungen sowie der durchgeführten Sicherung in Stichproben.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrollen ausreichend wirksam sowie geeignet sind, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

10.9 Service Level Management

Kontrollbeschreibung
SLA1 – Es wird sichergestellt, dass die durch vereinbarte Service Level Agreements (SLAs) gesetzten Parameter und Dienstleistungsvereinbarungen in geordneter Weise in den Regelbetrieb für die unterschiedlichen Dienstleistungen der Gesellschaft Einzug finden.

Kontroll ID	Segment	Kontrollbeschreibung	Prüfungshandlungen	Prüfungsergebnis
SLA1-1	CL	Vertraglich vereinbarte Dienstleistungen mit Kunden sind dokumentiert. Erfolgt die Dokumentation über SLAs sollten diese u. a. Definitionen, Bezugsgrößen, Messverfahren, Messpunkte und Messintervalle beinhalten.	Befragung der Prozessverantwortlichen bezüglich der Service Level Agreements (SLAs). Prüfung in Stichproben, ob die vertraglich dokumentierten Service Level Agreements (SLAs) entsprechende Inhalte wie Messkriterien, Messverfahren und Serviceklassen enthalten.	Keine Beanstandungen

Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrolle ausreichend wirksam sowie geeignet ist, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.

10.10 Physical and Logical Environmental Security

Kontrollbeschreibung				
PLS1 – Der Schutz der Hardware und Daten werden durch angemessen konzipierte und verwaltete Systeme sowie physische Einrichtungen unterstützt.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
PLS1-1	CS	Ein schriftliches Zutrittskonzept regelt den Schutzbedarf der Standorte und Räumlichkeiten. Daraus abgeleitete Sicherheitsanforderungen sind entsprechend des definierten Schutzbedarfs dokumentiert und umgesetzt.	Befragung der Prozessverantwortlichen bezüglich des Zutrittskonzepts und dessen Umsetzung. Überprüfung der dokumentierten Zugriffssicherheitspolitik und Prüfung, ob Sicherheitszonen wie beschrieben implementiert sind.	Keine Beanstandungen
PLS1-2	CL	Eine angemessene physische Sicherheit im Rechenzentrum der Gesellschaft ist gegeben. Physische Sicherheitsmaßnahmen zum Schutz der Hard- und Software umfassen u. a. - Bauliche Maßnahmen, - Zugangskontrollen, - Klimatisierungstechnik, - Feuerschutzmaßnahmen, - Maßnahmen zur Sicherung der Stromversorgung (USV, Notstromaggregat, Anbindung) sowie die regelmäßige Wartung der Anlagen.	Gespräch mit den verantwortlichen Mitarbeitern, Einsichtnahme in Dokumentationen sowie Begehung von Rechenzentren in Köln. Rundgang durch das Rechenzentrum und Prüfung der Sicherheitsmaßnahmen zum Schutz von Hard- und Software. Des Weiteren haben wir die Wartungsprotokolle in Stichproben geprüft.	Keine Beanstandungen

Kontrollbeschreibung				
PLS1 – Der Schutz der Hardware und Daten werden durch angemessen konzipierte und verwaltete Systeme sowie physische Einrichtungen unterstützt.				
Kontroll ID	**Segment**	**Kontrollbeschreibung**	**Prüfungshandlungen**	**Prüfungsergebnis**
PLS1-3	CL	Das unternehmensinterne Netzwerk ist über IT-Sicherheitsmechanismen wie z. B. Firewalls abgesichert und von den Netzwerken der Kunden getrennt. Zudem sind die einzelnen Kundennetzwerke voneinander getrennt.	Gespräch mit dem Prozessverantwortlichen und Einsichtnahme in entsprechende Netzwerkpläne. Prüfung von Netzwerkplänen, Routingtabellen und von ICMP-Anfragen, um festzustellen, ob interne Netzwerke gesichert und getrennt sind.	Keine Beanstandungen
PLS1-4	CL	Der externe Zugriff auf das Netzwerk der QSC AG ist für autorisierte Personen nur über gesicherte und verschlüsselte Kommunikationswegen (bspw. ein VPN möglich) möglich. Eine 2-Phasen-Authentifizierung ist erforderlich.	Gespräch mit dem Prozessverantwortlichen zu dem externen Zugriff auf das Netzwerk der QSC AG. Durchführung eines Walkthroughs und Prüfung, dass eine 2-Phasen-Authetifizierung erforderlich ist.	Keine Beanstandungen
Auf Grundlage der oben dargestellten Prüfungshandlungen kommen wir zu dem Ergebnis, dass die Kontrollen ausreichend wirksam sowie geeignet sind, um das Kontrollziel mit hinreichender Sicherheit zu erreichen.				

Anlagen
Allgemeine Auftragsbedingungen

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im Nachstehenden zusammenfassend „Wirtschaftsprüfer“ genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies ausdrücklich vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags schriftlich darzustellen hat, ist alleine diese schriftliche Darstellung maßgebend. Entwürfe schriftlicher Darstellungen sind unverbindlich. Sofern nicht anders vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie schriftlich bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt.

(3) Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

(4) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

(5) Ein einzelner Schadensfall im Sinne von Abs. 2 ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(6) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und

d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.