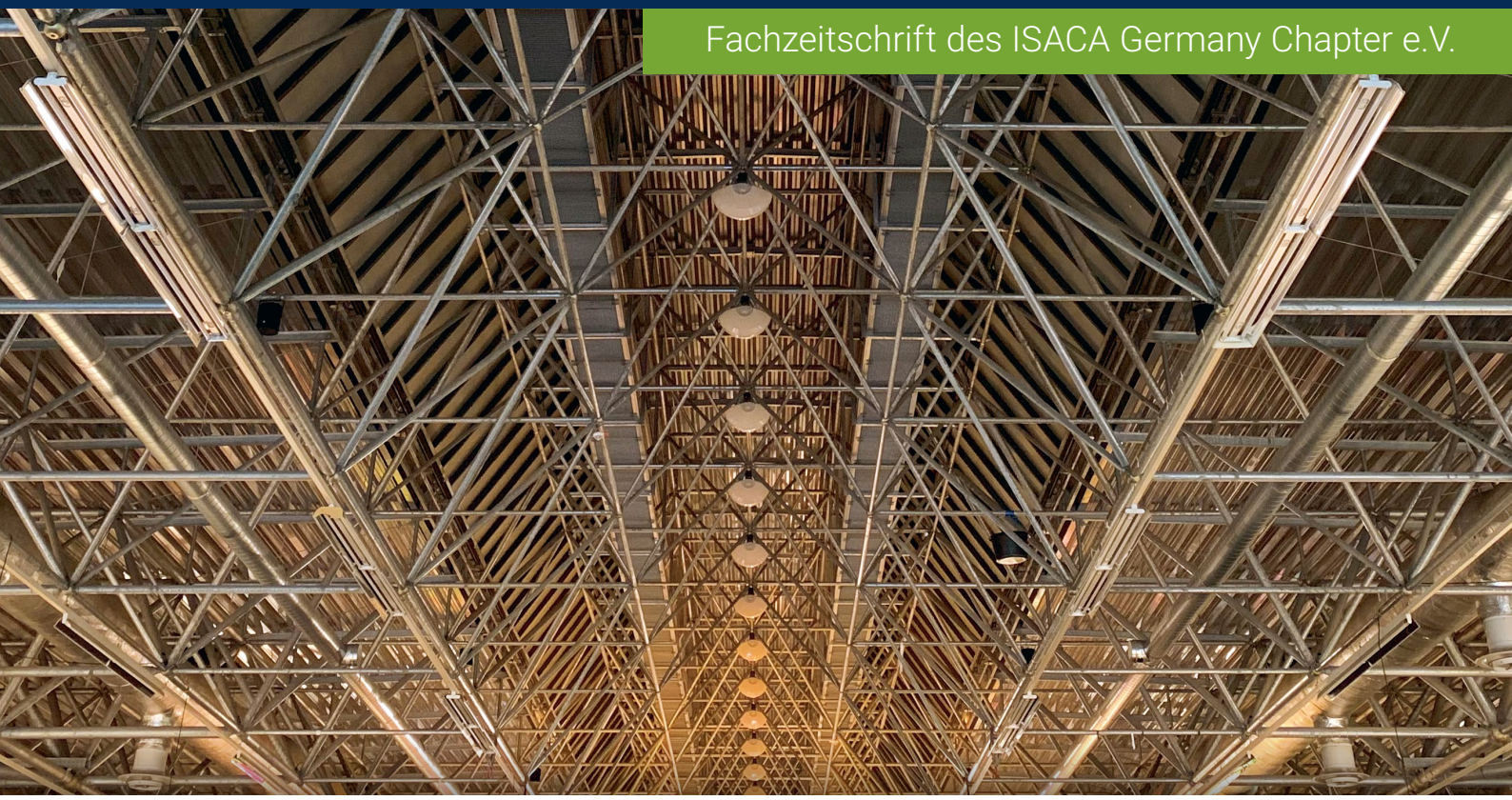
Heft 32 | Dezember 2020 | 14. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e.V.



IT-Prüfung

IT-Prüfungen außerhalb von Abschlussprüfungen – Kriterien für eine Prüfung nach PS 860

Martin Fröhlich

Sonderdruck

ISACA Germany Chapter

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

Sonderdruck
aus:

IT-Governance
Fachzeitschrift des ISACA Germany Chapter e.V.

http://it-governance.dpunkt.de/

14. Jahrgang – Heft 32 – Dezember 2020
Seiten 23–24

ISSN 1864-6557

IT-Prüfung
IT-Prüfungen außerhalb von Abschlussprüfungen – Kriterien für eine Prüfung nach PS 860

Martin Fröhlich

Die zunehmende Digitalisierung von Geschäftsprozessen sowie die Abhängigkeit der Unternehmen und der Gesellschaft von funktionsfähigen und zuverlässigen Infrastrukturen erhöhen die Nachfrage nach Bestätigungsleistungen, ob die verwendeten Technologien, Prozesse und Verfahren im Hinblick auf den vorgesehenen Einsatzzweck geeignet sind und die damit verbundenen Sicherheits- und Compliance-Anforderungen erfüllt werden. Um diese Nachfrage nach Bestätigungsleistungen zu erfüllen und sich gleichzeitig von am Markt anzutreffenden »Zertifizierungen« abzugrenzen, hat das Institut der Wirtschaftsprüfer mit dem Prüfungsstandard »IT-Prüfungen außerhalb der Abschlussprüfung« (PS 860) [IDW PS 860] ein Rahmenwerk verabschiedet, das als Basis für die Prüfung unterschiedlicher Technologien und Anwendungsfälle herangezogen werden kann. Gegenüber anderen »Assurance-Leistungen« zeichnet sich der PS 860 durch einen strikt an Kriterien orientierten Prüfungsansatz, eine definierte Prüfungsmethodik und transparente Berichtsformate aus (vgl. hierzu ausführlich [Campe & Riedel 2020]).

Erläuterung der Prüfungshinweise

Der PS 860 in seiner Rolle als Dachstandard wird konkretisiert durch Prüfungshinweise (PH), die Mindestkriterien enthalten, die vom Geprüften beachtet werden müssen. Diese werden ergänzt um Grundsätze, Verfahren und Maßnahmen zur Umsetzung dieser Kriterien und beispielhafte Prüfungshandlungen des Wirtschaftsprüfers. Im Sinne einer transparenten Berichterstattung sind jedem Prüfungshinweis Berichtsmuster beigefügt, die auf die verschiedenen Arten[1] der Prüfungen abgestimmt sind.

Im Folgenden werden die bereits veröffentlichten und die vor einer Veröffentlichung stehenden Prüfungshinweise kurz erläutert und im Hinblick auf ihren Anwendungsbereich eingeordnet.

Bereits im Juni 2018 wurde der erste Prüfungshinweis PH 9.860.1 zur Prüfung einer gesetzesadäquaten Datenschutzorganisation veröffentlicht [IDW PH 9.860.1]. In Anlage 1 enthält der PH 9.860.1 einen umfangreichen Katalog an Grundsätzen, Verfahren und Maßnahmen zu den jeweiligen Anforderungen der Datenschutz-Grundverordnung (DSGVO). Die Grundsätze, Verfahren und Maßnahmen wurden von Praktikern entwickelt, die langjährige Prüfungs- und Beratungserfahrungen auf dem Gebiet der Datenschutzorganisation haben. Diese Grundsätze, Verfahren und Maßnahmen können dem Unternehmen wertvolle Hinweise bei der Einrichtung einer gesetzeskonformen Datenschutzorganisation geben. Eine Prüfung nach PH 9.860.1 kann zudem die Grundlage für eine datenschutzspezifische Zertifizierung gemäß Art. 42 DSGVO bilden.

Im Juni 2019 wurde der PH 9.860.2 über die Prüfung von Betreibern kritischer Infrastrukturen veröffentlicht [IDW PH 9.860.2]. Dieser Prüfungshinweis richtet sich in erster Linie an den Prüfer von Betreibern kritischer Infrastrukturen. Er referenziert auf die Anforderungen des BSI-Dokuments »Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen« (Stand 28.02.2020) [BSI 2020] und beschreibt zu jeder Anforderung Prüfungshandlungen zur Beurteilung der Angemessenheit sowie zur Prüfung der Wirksamkeit. Mit der Beurteilung der Angemessenheit prüft der Wirtschaftsprüfer, ob eine Anforderung adäquat ausgestaltet und implementiert ist; die Beurteilung der Wirksamkeit richtet sich auf die Einhaltung der Maßnahmen im Prüfungszeitraum.

Im Mai 2020 wurde der dritte Prüfungshinweis mit dem Titel »Die Prüfung von Cloud-Diensten« veröffentlicht [IDW PH 9.860.3]. Auch dieser PH wendet sich in erster Linie an Wirtschaftsprüfer, die Cloud-Services prüfen. Der PH unterscheidet hinsichtlich der Anforderungen und beispielhaften Prüfungshandlungen zwischen drei Betreibermodellen für Cloud-Services:

- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)

Als Grundlage für die Beurteilung von IaaS wird der Anforderungskatalog C5 des BSI herangezogen [BSI 2016]. Zu jeder Anforderung ist vermerkt, ob aus Sicht eines Wirtschaftsprüfers die Basisanforderungen oder auch die optionalen weitergehenden Anforderungen beachtet werden müssen. Die Anforderungen basieren noch auf dem Stand 2016 des BSI C5. Eine Anpassung auf den aktuellen Stand 2020 ist für 2021 geplant.

Für die Betreibermodelle PaaS und SaaS sind in den Kapiteln 18 ff. über den C5 hinausgehende Anforderungen definiert, die sich an den Rechnungslegungsstandards RS FAIT 1 [IDW RS FAIT 1] und RS FAIT 5 [IDW RS FAIT 5] orientieren.

1 Direkte Prüfung vs. Prüfung einer Erklärung, Prüfung der Angemessenheit vs. Prüfung der Wirksamkeit, vgl. [Campe & Riedel 2020, S. 319].

Auch für den PH 9.860.2 sowie den PH 9.860.3 hat der Fachausschuss für Informationstechnologie (FAIT) auf die Unterstützung erfahrener Praktiker in der Prüfung kritischer Infrastrukturen und Cloud-Services zurückgegriffen.

Derzeit in der Entwicklung ist ein neuer Prüfungshinweis über die Prüfung der Einhaltung der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) und somit der steuerrechtlichen Anforderungen an die Ordnungsmäßigkeit und Sicherheit von rechnungslegungsrelevanten Daten und IT-Systemen.

Sowohl die Technologien als auch das Bedürfnis nach Bestätigungsleistungen werden sich weiterentwickeln. Analog hierzu wird es neben einer Weiterentwicklung des PS 860 in Zukunft auch weitere Prüfungshinweise zur Prüfung neuer Technologien und IT-Systeme geben ◗

Martin Fröhlich

ist CISA, CGEIT, IT-Auditor[IDW] und berät Unternehmen rund um die Themen IT-Governance und IT-Compliance. Vor der Gründung seiner Firma IT-Compliance Solutions war er jahrzehntelang Mitarbeiter der Wirtschaftsprüfungsgesellschaft PwC, davon 20 Jahre Partner mit der Verantwortung für die Prüfung und Beratung von Finanzdienstleistungsunternehmen. Martin Fröhlich ist Mitglied des FAIT beim IDW und Vizepräsident des ISACA Germany Chapter e. V.

Dr. Martin Fröhlich
IT-Compliance Solutions
Kerkmannstr. 6
46535 Dinslaken
info@martin-froehlich.de
https://martin-froehlich.de/

Literatur

[BSI 2016] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* BSI Anforderungskatalog Cloud Computing (C5), Stand 2016; *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2016/Anforderungskatalog-Cloud_Computing-C5.pdf?__blob=publicationFile&v=1*, Zugriff am 25.09.2020.

[BSI 2020] *Bundesamt für Sicherheit in der Informationstechnik (BSI):* Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen, Stand 28.02.2020.

[Campe & Riedel 2020] *Campe, P.; Riedel, O.:* IT-Prüfung außerhalb der Abschlussprüfung – Ein Überblick über Kerninhalte von IDW PS 860. WPg, Heft 6, 2020, S. 317-323.

[IDW PH 9.860.1] *Institut der Wirtschaftsprüfer (IDW):* IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1), Stand 19.06.2018.

[IDW PH 9.860.2] *Institut der Wirtschaftsprüfer (IDW):* IDW Prüfungshinweis: Die Prüfung der von Betreibern kritischer Infrastrukturen gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2), Stand 21.06.2019.

[IDW PH 9.860.3] *Institut der Wirtschaftsprüfer (IDW):* IDW Prüfungshinweis: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3), Stand 15.05.2020.

[IDW PS 860] *Institut der Wirtschaftsprüfer (IDW):* IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860), Stand 02.03.2018.

[IDW RS FAIT 1] *Institut der Wirtschaftsprüfer (IDW):* IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1), Stand 24.09.2002.

[IDW RS FAIT 5] *Institut der Wirtschaftsprüfer (IDW):* IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (IDW RS FAIT 5), Stand 04.11.2015.

»IT-Governance« – Aims & Scope

»IT-Governance« adressiert die Herausforderungen des modernen IT-Managements und vermittelt aktuelles Wissen über wegweisende und beispielhafte Methoden, Konzepte und Erfolgsfaktoren der IT-Governance für Management, Berater, Auditoren und Wissenschaftler. Die Artikel umfassen Überblicksdarstellungen, Analysen, Forschungsergebnisse, Fallstudien, Success Stories und Tutorials. Sie sind praxisorientiert und reflektieren theoretische Konzepte sowie den aktuellen Stand der Forschung. Einen Schwerpunkt der Beiträge bilden einerseits Informationen rund um das Referenzmodell »Control Objectives for Information and related Technology« (COBIT), andererseits Ergebnisse, die in den ISACA-Arbeitskreisen erzielt werden.

Ein Serviceteil enthält außerdem Informationen zu Standards, IT-Prüfung und neuen Büchern aus dem Themenumfeld der IT-Governance.

»IT-Governance« ist die Fachzeitschrift des Germany Chapter der »Information Systems Audit and Control Association« e.V. (ISACA).

»IT-Governance« wird herausgegeben von
Dr. Martin Fröhlich
Prof. Dr. Matthias Goeken
Prof. Dr. Michael Klotz
Ingo Struckmeyer
(verantwortlicher Schriftleiter)
Marc Weber
(hrsg-itgov@dpunkt.de)