IT- Systemprüfung gemäß IDW PS 330, dem neuen ITSiG, den Anforderungen der neuen EU-DS-GVO sowie der Vorbereitung auf die neuen Anforderungen der GOBD

Zweck/Aufgabe

Feststellung der Ordnungsmäßigkeit, Sicherheit und Nachvollziehbarkeit der installierten Informationstechnologie in der Jahresabschlussprüfung und Beachtung der gesetzlichen Anforderungen

1. Ausgangssituation

Berufsrechtliche und gesetzliche Anforderungen

Der Abschlussprüfer hat das IT-gestützte Rechnungslegungssystem daraufhin zu beurteilen, ob es den gesetzlichen Anforderungen und insbesondere den Ordnungsmäßigkeits- und Sicherheitsanforderungen entspricht, um die nach § 322 Abs. 1 Satz 1 HGB i. V. m. § 317 Abs. 1 Satz 1 HGB und § 321 Abs. 2 Satz 2 HGB geforderten Prüfungsaussagen über die Ordnungsmäßigkeit der Buchführung zu erfüllen. Folglich hat der Abschlussprüfer das IT-System des Unternehmens insoweit zu prüfen, als dessen Elemente dazu dienen, Informationen über Geschäftsvorfälle abzubilden, die für die Rechnungslegung von Bedeutung sein können (rechnungslegungsrelevant). Der Begriff der Rechnungslegung umfasst dabei die Buchführung, den Jahresabschluss und den Lagebericht bzw. auf Konzernebene den Konzernabschluss und den Konzernlagebericht. (Auszug aus IDW PS 330)

Darüber hinaus wurden auch die gesetzlichen Anforderungen an die Sicherheit der Informationstechnologie durch die Neuregelung des IT-Sicherheitsgesetzes (ITSiG) deutlich verschärft. Ferner wurde der Nachweis der Ordnungsmäßigkeit nicht nur auf die führenden Finanz- bzw. Rechnungslegungsprogramme begrenzt, sondern erstreckt sich nach den GoBD auch auf die Datenhaltung und Informationsbereitstellung der vor- und nachgelagerten Systeme sowie rechnungslegungsrelevanten Nebensysteme.

Bei der heutigen Komplexität der installierten IT-Systeme, der IT-Infrastruktur, der IT-Organisation, der IT-Anwendungssysteme und der digital gespeicherten Massendaten ist es für den Prüfer ohne technische Hilfsmittel nicht mehr möglich, innerhalb der Abschlussprüfung und in angemessener Zeit die erforderliche Ordnungsmäßigkeit der Informationstechnologie festzustellen, zu beurteilen und zu dokumentieren.

Aus den in einer Vielzahl im Dienste der Wirtschaftsprüfung und Revision durchgeführten IT-Systemprüfungen hat REVIDATA GmbH deshalb auf Grundlage des IDW PS 330 ein Prüfungswerkzeug, den REVIDATA-Prüfungswürfel entwickelt und über die Jahre kontinuierlich verbessert. Diese Weiterentwicklung unseres Prüfungswürfels betrifft auch die stetige Ergänzung der neuen Anforderungen, welche in den letzten Jahren durch neue Bestimmungen und Verordnungen wie beispielsweise ITSiG, GoBD, OwiG und EU-DS-GVO gefordert werden.

2. Zielsetzung

REVIDATA Lösung für Wirtschaftsprüfung und Revision

Mit dem Einsatz des REVIDATA-*Prüfungswürfels* soll es dem Abschlussprüfer ermöglicht werden, selbst komplexe Informationssysteme entsprechend der gesetzlichen und berufsrechtlichen Anforderungen in angemessener Zeit effizient zu prüfen, zu beurteilen und die Feststellungen und die Prüfungsergebnisse zu dokumentieren. Darüber hinaus soll REVIDATA GmbH eine fachliche Unterstützung durch ihre eigenen IT-Prüfer sicherstellen.

3. Durchführung

3.1 Prüfungsvorbereitung

In einem vorbereitenden Gespräch wird der verantwortliche Mitarbeiter des Mandanten über den Zweck, die Art und den Umfang der geplanten IT-Prüfung informiert und die Terminierung verabredet. Er erhält zur Vorbereitung der IT-Systemprüfung von REVIDATA die Checkliste IDW PH 330.1, welche dem IDW PS 330 entsprechend in 9 Gruppen unterteilt und zusätzlich um die Gruppen 10 und 11 zur Prüfung des Datenschutzes und der Vorbereitung zu den Anforderungen der GoBD erweitert ist.

1. Prüfung der Unternehmens-/IT-Strategie (IDW PS 330, Tz. 51 f.)
2. Prüfung des IT-Umfeldes (IDW PS 330, Tz. 51 f.)
3. Prüfung der IT -Organisation (IDW PS 330, Tz. 51 f.)
4. Prüfung der IT-Infrastruktur (IDW PS 330, Tz. 53 ff.)
5. Prüfung der IT-Anwendungen (IDW PS 330, Tz. 70 ff.)
6. Prüfung IT-gestützter Geschäftsprozesse (IDW PS 330, Tz. 84 ff.)
7. Prüfung des IT-Überwachungssystems (IDW PS 330, Tz. 89)
8. Prüfung des IT-Outsourcings (IDW PS 330, Tz. 90 ff.)
9. Besonderheiten der Internetnutzung

Zusätzlich ergänzte Prüfbereiche

10. Vorbereitung und Einhaltung der Datenschutzgesetzgebung
11. Vorbereitung und Einhaltung der GoBD (Abgabenordnung)

Diese Checkliste dient als Bestandsaufnahme für die von dem IT-Verantwortlichen des Mandanten zu erstellende zusammenfassende Darstellung der bei dem Mandanten vorhandenen und prüfungsrelevanten Unterlagen und Informationen. Zusätzlich werden Unterlagen angefordert, die Auskunft darüber geben sollen, inwieweit die Organisation und das Management des Mandanten auf die Anforderungen der GOBD und des Datenschutzes vorbereitet ist.

3.2 Bestandsaufnahme und Bewertung

Die von dem Mandanten bearbeitete Checkliste mit den zusätzlich gelieferten Unterlagen und Informationen werden von dem IT-Prüfer gesichtet, geordnet und hinsichtlich ihrer für die Prüfung notwendige Vollständigkeit und Verständlichkeit geprüft und im Zweifelsfalle möglichst telefonisch vervollständigt.

3.3 Prüfungsdurchführung

In einer Begehung mit Sichtung weiterer Unterlagen und der Organisation sowie der Einholung noch benötigter Informationen werden die für die Prüfung erforderlichen Prüfungshandlungen durchgeführt. Danach werden sämtliche Feststellungen der Prüfung gemäß der Ordnung der IDW PH 330.1-Checkliste in den REVIDATA-Prüfungswürfel übernommen. Der Prüfer kennzeichnet dabei den Erfüllungsgrad jedes Prüfungspunktes mit „ja“, „nein“ oder „teilweise erfüllt“.

Die hinterlegte Systematik des REVIDATA-Prüfungswürfels prüft im Folgenden die Vollständigkeit der bearbeiteten Prüfungsfragen und bewertet nach ebenfalls hinterlegten statistisch/wissenschaftlichen Formeln den Erfüllungsgrad der IT-Systeme des Mandanten mit der im IDW PS 330 aufgestellten Anforderung an eine ordnungsgemäße Informationstechnologie. Darüber hinaus erstellt der REVIDATA-Prüfungswürfel

- den Berichtsentwurf,
- die ausgefüllte und bewertete IDW PH 330.1-Checkliste,
- die bewertete und priorisierte Mängelliste und
- eine mit einer statistischen Eintrittswahrscheinlichkeit berechnete Mängelliste.

4. Ergebnis

Als Ergebnis wird ein Prüfbericht mit den Feststellungen der analysierten Abweichungen zwischen den physischen Unternehmensprozessen und den entsprechenden DV-Geschäftsprozessen zur Darstellung der Abweichungsursachen sowie ein abgestimmter Maßnahmenplan mit Risikoeinstufung zur Fehlerbeseitigung übergeben.

Mithilfe dieser Informationen soll es dem Abschlussprüfer möglich sein, zusätzlich erforderliche Kontroll- und Sicherheitsmaßnahmen zu definieren, um zukünftig zwischen den physischen Unternehmensprozessen und den Daten der IT-Systeme eine inhaltliche und nachvollziehbare Stimmigkeit zu gewährleisten.

5. Nutzen

Mit der Unterstützung der REVIDATA GmbH und mit dem standardisierten Vorgehensmodel der REVIDATA wird es dem Abschlussprüfer ermöglicht, in angemessener Zeit alle Prüfungshandlungen auf Grundlage des IDW PS 330 nachvollziehbar durchzuführen und zusätzlich festzustellen inwieweit der Mandant auf die Anforderungen des Datenschutzgesetzes und der Abgabenordnung (GoBD) vorbereitet ist.

Zusätzlich erhält der Abschlussprüfer Informationen zur Feststellung sonstiger Auffälligkeiten in der IT-Infrastruktur, der Informationsverarbeitung, den Anwendungen, den Prozessen und der IT-Sicherheit, welche die Ordnungsmäßigkeit der Informationstechnologie (IDW PS 330, IDW PS 880), die Organisation (IDW PS 261), den Datenschutz (EU-DS-GVO), die Abgabenordnung (GoBD) und das IT-Sicherheitsgesetz (ITSiG) tangieren könnten.
Bei erkannten Risiken ergeben sich Ansätze für weitere erforderliche Beratungstätigkeiten zur Mandantensicherheit.

Der Mandant erhält eine qualifizierte Übersicht der in seinen Geschäftsprozessen auffälligen IT-technischen und organisatorischen Risiken und deren Bewertung zur Eintrittswahrscheinlichkeit.

Als erweiterte Dienstleistungen bietet REVIDATA GmbH:

- Auffälligkeitsanalyse und Beurteilung des Datenbestandes (Auffälligkeitsscan IDW PS 210/PH 9.330.3)
- Tiefenanalyse der Geschäftsprozesse zur neuen GoBD
- Sicherstellung der organisatorischen Anforderungen der neuen EU-DS-GVO
- Tiefenprüfung der Einhaltung der gesetzlichen Anforderungen aus dem neuen IT-SiG

6. Glossar

IT-SiG	IT-Sicherheitsgesetz
OwiG	Ordnungswidrigkeitsgesetz
AO	Abgabenordnung
HGB	Handelsgesetzbuch
GOBD	Grundsätze ordnungsmäßiger Buchhaltung
IDW PS 330	Prüfungsstandard der IT-Informationstechnologie
IDW PH 9.330.1	Empfohlene Checkliste zur Prüfung der Informationstechnologie
IDW PS 210	Analyse des Datenbestandes in der Abschlussprüfung
IDW PH 9.330.3	Empfohlene Analyse des Datenbestandes in der Abschlussprüfung
IDW PS 261	Prüfung des IKS
IDW PS 880	Prüfung der ordnungsmäßigen Software Entwicklung/Release Wechsel
EU-DS-GVO	Europäische Datenschutz-Grundverordnung

7. Kontakt

REVIDATA GmbH
Tel.: +49 211 49690-0
Fax: +49 211 49690-29
E-Mail: info@revidata.de
Home: www.revidata.de

Wir freuen uns auf Ihre geschätzte Kontaktaufnahme!