Erfahrung nutzen, Zukunft sichern.

DIIR Deutsches Institut für Interne Revision e.V.

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 71 37 69 - 0
Fax (069) 71 37 69 - 69
www.diir.de
info@diir.de
USt-ID DE 114235123

DIIR – Deutsches Institut für Interne Revision e.V. Ohmstraße 59 60486 Frankfurt am Main

Institut der Wirtschaftsprüfer
in Deutschland e.V.
Tersteegenstraße 14
40474 Düsseldorf

Frankfurt am Main
26. Februar 2010

**Neufassung des IDW Prüfungsstandards IDW EPS 880**

Sehr geehrte Damen und Herren,

leider ist uns eine Teilnahme an der Anhörung zum Entwurf der Neufassung des IDW Prüfungsstandards „Die Prüfung von Softwareprodukten (IDW EPS 880 n. F.)" nicht möglich. Dennoch möchten wir Ihnen gerne anbei eine Reihe von Anmerkungen zukommen lassen und hoffen, dass diese Ihnen noch einige nützliche Anregungen geben können.

Mit freundlichen Grüßen

DIIR – DEUTSCHES INSTITUT FÜR INTERNE REVISION e.V.
Die Geschäftsführung

(V. Hampel)

Anlage



Commerzbank AG
BLZ 500 400 00
Konto 5 892 807
IBAN DE85 5004 0000 0589 2807 00
BIC COBA DE FF 500

Dresdner Bank AG
BLZ 500 800 00
Konto 93 258 900
IBAN DE56 5008 0000 0093 2589 00
BIC DRES DE FF

Postbank Frankfurt
BLZ 500 100 60
Konto 88 068 604
IBAN DE06 5001 0060 0088 0686 04
BIC PBNK DE FF

Stellungnahme zum Entwurf der Neufassung des IDW Prüfungsstandards 880 (Die Prüfung von Softwareprodukten)

| Textziffer | Seite | Anmerkung |
|---|---|---|
| 10 | 4 | Wir empfehlen festzustellen, inwiefern eine Verfahrensdokumentation überhaupt vorhanden ist bzw. insbesondere zu prüfen, ob diese aktuell ist.<br><br>Begründung: das Fehlen der Verfahrensanweisung oder der mangelnde Bezug zum aktuellen Stand der Prozeduren stellt einen Mangel in Bezug auf die Nachvollziehbarkeit der Systemverfahren dar. |
| 16 | 4 | Wir empfehlen kurze weitergehende Erläuterungen zum Begriff „sachgerecht".<br><br>Begründung: es sollte erwogen werden, einzelne Kriterien exemplarisch in Bezug auf die Anwendung zu definieren, anhand derer eine sachgerechte Anwendung ermöglicht wird. Dies könnten bspw. nachweisliche und nachvollziehbare Schulungen oder Bedienungsunterlagen sein, die ihrerseits die Risiken einer unsachgemäßen Anwendung reduzieren oder sogar ausschließen. |
| 18 | 5 | Es könnte erwogen werden, neben § 25 KWG exemplarisch auch die recht stringenten Anforderungen des MaRisk an das Risikomanagement zu erwähnen. |
| 32 | 7 | Wir empfehlen, als Prüfungskriterium auch die Einbettung der Systeme in die operativen Geschäftsprozesse zu untersuchen. Gegenstand kann das Vorhandensein geeigneter operativer Organisationsanweisungen, Rollendefinitionen der Anwender etc. sein.<br><br>Begründung: Grundsätzlich ist die Sicherheit der rechnungsrelevanten IT-Systeme und Daten auch maßgeblich abhängig von den operativen Geschäftsprozessen. |
| 32 | 8 | Wir empfehlen, folgenden Punkt ggf. noch zu ergänzen:<br>• Adäquate, den geltenden Anforderungen entsprechende Parametrisierung des Systems.<br><br>Begründung: die Überprüfung der Sicherheit sollte auf nachvollziehbarer Basis der aktuellsten operativen Anforderungen erfolgen |
| 48 | 11 | Wir empfehlen, auch einen Bezug zur Entwicklungsplattform herzustellen (bspw. auch Java, .net, etc)<br><br>Begründung: die eingesetzte Entwicklungsplattform kann aufgrund ihrer Spezifika ggf. besonders beachtenswerte Prüfungsgegenstände implizieren. |
| 52 | 12 | Wir empfehlen, bei „Kontrollumfeld" folgenden Risikoindikator noch zu ergänzen:<br>• Mangelnde Kenntnisse über die rechtlichen bzw. aufsichtsrechtlichen Anforderungen.<br>Bei „Softwarentwicklungsumgebung" sollte als Risikoindikator noch ergänzt werden:<br>• Unzureichende Versionierung<br>• Unzureichende Programmübernahmeverfahren<br>Bei „Technologie" lässt der genannte Risikoindikator „Verwendung veralteter Technologie" einen erheblichen Ermessensspielraum. Danach wäre u. U. eine Programmierung in „Cobol" in einer Großrechnerumgebung veraltet und damit risikobehaftet. Treffender wäre folgender Ausdruck:<br>• Verwendung komplexer, inhomogener und/oder unausgereifter Technologien |

Stellungnahme zum Entwurf der Neufassung des IDW Prüfungsstandards 880 (Die Prüfung von Softwareprodukten)

| Textziffer | Seite | Anmerkung |
|---|---|---|
| 68 | 16 | Wir empfehlen, die Formulierung des ersten Anstriches zu ändern:<br>• Alle **wesentlichen** Programmfunktionen durch Testfälle abgedeckt werden.<br><br>Begründung: der Ausdruck „alle Programmteile durch Testfälle abgedeckt werden" induziert eine 100% Abdeckung beim Test, die in der Realität jedoch kaum erreicht werden kann.<br><br>Beim 2. Spiegelstrich sollten auch „Lasttests" Erwähnung finden. |
| 79/80 | 18 | Wir empfehlen, wo möglich, Konkretisierungen vorzunehmen. Bspw. ist nicht klar, wie sich Mängel im Umfeld der Programmentwicklung auf das Urteil auswirken.<br><br>Begründung: mit einigen praktischen Handlungsempfehlungen könnte den Prüfern weitere Unterstützung geboten werden. Folgendes Beispiel hierzu: wie ist es zu werten, wenn der Test unzureichend war oder nicht geeignete Technologien verwendet wurden? |
| 105 | 22 | Wir empfehlen, hier weitere Konkretisierungen in Bezug auf Softwarestand und –parametrisierung vorzunehmen.<br><br>Begründung: es kommt in entscheidendem Maße auch darauf an, wie die Software beim Anwender implementiert ist. Auch eine Software mit Bescheinigung kann beim Anwender so parametrisiert sein, das sie nicht mehr ordnungsgemäß ist (z. B. alle User im SAP-System haben eine SAP_ALL-Berechtigung). |