Zertifizierung nach IDW PS 880

Gefährdungsanalyse, Kontrollplanung, MAR kompakt

Vertrauen ist gut. Kontrolle ist besser. Wenn Sie auslagern, geben Sie einen Vertrauensvorschuss. Es ist die Aufgabe des Insourcers, Ihnen überprüfbare und nachvollziehbare Kriterien zu liefern, warum eine Auslagerung ein kalkulierbares Risiko ist. Wir kommen dem u. a. mit der Zertifizierung unserer Anwendungen nach IDW PS 880 nach.

Für die Erfüllung der Compliance-Funktion gemäß MaRisk AT 4.4.2. bedarf es in erster Linie

- des aufsichtsrechtlichen Kow-hows,
- der Kenntnis des Beauftragten über die (auslagernde) Bank,
- der richtigen Schlussfolgerungen des Beauftragten zur Risikosituation und zu den abzuleitenden sowie zu kontrollierenden Präventionsmaßnahmen und am Ende
- einer nachvollziehbaren und revisionssicheren Dokumentation der Tätigkeit.

Bei diesen Aufgabe werden die Beauftragten – Ihre ausgelagerten Beauftragtenfunktionen – mit unterschiedlichen Anwendungen unterstützt.

Diese Anwendungen sind zugleich Voraussetzung und Ausdruck des Mehrmandantenansatzes: Ohne die Anwendungen könnten wir die Beauftragtenfunktionen weder so transparent noch so günstig anbieten. Ohne diese Anwendungen wäre aber auch das vergleichsweise hohe Sicherheits- und Qualitätsniveau nicht erreichbar.

Von der elektronischen Akte zum Analysetool

Bislang standen bei der technischen Unterstützung des Beauftragten eine effiziente Bearbeitungs- sowie Auswertungs- und Steuerungsmöglichkeit im Vordergrund. In der jüngeren Vergangenheit wurden in den Anwendungen zudem mehr und mehr systematische Analysen integriert. Sie helfen dem Beauftragten bei der Einschätzung komplexerer Sachverhalte oder geben Entscheidungsvorschläge für Risikobeurteilungen. Analysen und Berechnungen erfolgen nach bestimmten zentral erarbeiteten fachlichen Kriterien und unter Einbeziehung unterschiedlicher Datenquellen.

Damit kommt der Anwendung selber, ihrer Angemessenheit und ihrer Funktionsfähigkeit eine deutlich größere Bedeutung zu.

Vor diesem Hintergrund und auch auf Basis unseres Qualitätsanspruchs haben wir uns entschlossen, unsere IT-Systeme zur

- systematischen Analyse von Wertpapiertransaktionen (MAR kompakt),
- Erstellung von Gefährdungsanalysen sowie
- risikoorientierten Kontrollplanungen

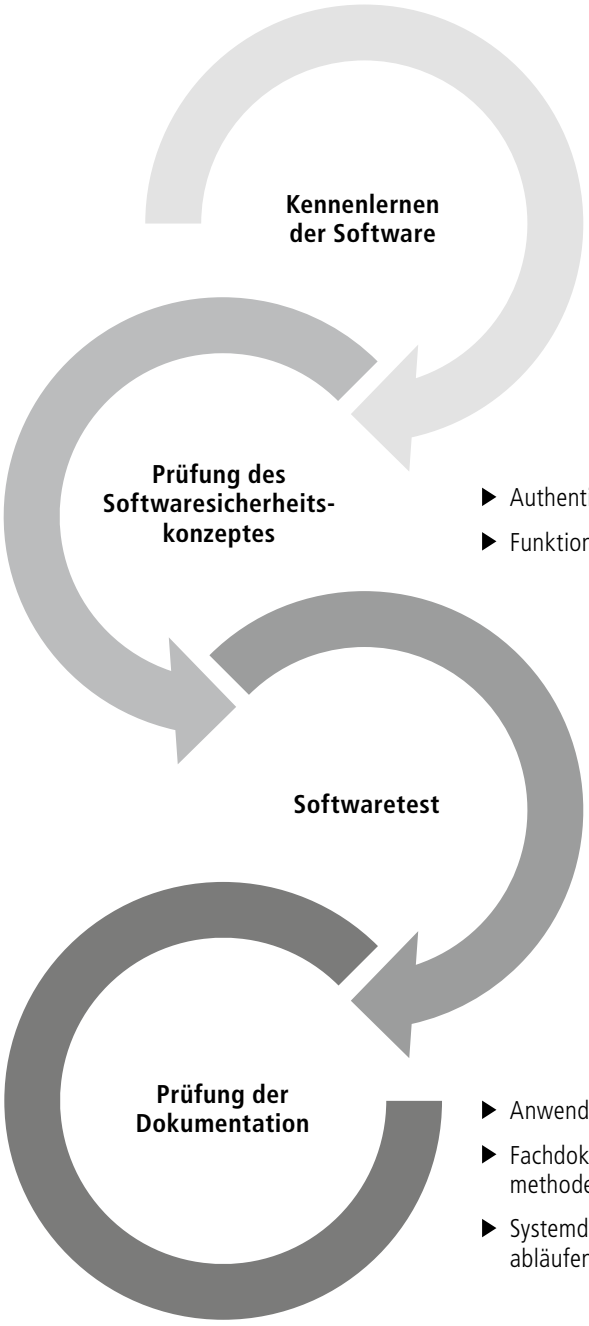
einer Zertifizierung gemäß dem Standard IDW PS 880 (siehe Abbildung auf Seite 19) zu unterwerfen. Diese Zertifizierung ergänzt unsere Zertifizierung nach IDW PS 951 Typ 2.

Eine gute Investition

Eine Zertifizierung ist zeitlich und aufwandstechnisch anspruchsvoll. Den Aufwand sehen wir aber als ein gutes Investment in die Zukunftsfähigkeit der IT-Anwendungen und damit mittelbar auch in die Zukunftsfähigkeit unserer Dienstleistungserbringung. Das Zertifikat bestätigt, dass die Anwendung (nach IDW PS 880) sicher ist – der Anwender, der Beauftragte und die auslagernde Bank können ihr vertrauen. Dabei war uns wichtig, ein Testat von unabhängiger Stelle, in diesem Fall von der Wirtschaftsprüfungsgesellschaft Ernst & Young GmbH, zu erhalten.

Und so haben wir abgeschnitten:

- Systematische Analyse von Wertpapiertransaktionen (MAR kompakt) – Testat uneingeschränkt erteilt.
- Gefährdungsanalyse – Testat uneingeschränkt erteilt.
- Risikoorientierte Kontrollplanung – Testat uneingeschränkt erteilt.



- Benennung der Ansprechpartner
- Benennung des Anwendungszwecks
- Benennung der Anwendungszielgruppe
- Bearbeitung des Anforderungskatalogs
- Bearbeitung des Funktionskatalogs
- Entwicklung des Testplans

- Authentifizierungsmechanismen
- Funktionstrennung

- Definierte Stichprobe
- Definierter Sollzustand
- Einhaltung der Verarbeitungsfunktionen
- Einhaltung der Programmabläufe
- Plausibilitätskontrollen

- Anwenderdokumentation
- Fachdokumentation zu den Berechnungs-methoden und -verfahren
- Systemdokumentationen zu Verfahrens-abläufen, Datenstrukturen und Schnittstellen

Die Anwendungsentwicklung findet in der GenoTec auf Initiative der jeweiligen Fachabteilungen und in der Regel unter Einbeziehung von Primärinstituten statt. Darüber hinaus stimmen wir uns mit dem Fachbeirat Beauftragtenwesen ab, der die Sicht der fünf Regionalverbände schon frühzeitig in die Anwendungsentwicklung einbringt. Neben der obligatorischen Prüfung des internen Kontrollsystems (IDW PS 951, Ausnahme IT-Sicherheit) beinhaltet die Zertifizierung nach IDW PS 880 ebenfalls die Prüfung der Angemessenheit der Programmfunktionen. Es wird geprüft, ob in der Anwendung die notwendigen Kriterien oder rechtlichen Rahmenbedingungen fachlich angemessen und korrekt umgesetzt wurden. Dies ist insbesondere wichtig bei der Umsetzung neuer aufsichtsrechtlicher Vorgaben, wie z. B. der MAR. >

Sie als auslagernde Bank können mit dem Testat sicher sein, dass

a. die Anwendung Daten korrekt verarbeitet und
b. die Rechenlogik die richtigen Ergebnisse unter Berücksichtigung relevanter Kriterien darstellt.

Relevante Kriterien sind **allgemeine** rechtliche Grundsätze und Richtlinien, u. a.:

- allgemeine Vorschriften
  - Handels- und steuerrechtliche Vorschriften für die Buchhaltung (§§ 238 ff. HGB und §§ 145 ff. AO)
  - branchenspezifische Vorschriften (z. B. KWG, MaRisk, WpHG, GWG, BDSG)
- prüfungsrelevante Vorschriften des Instituts der Wirtschaftsprüfer (IDW)
  - Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)
  - Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)
- zertifizierungsrelevante Vorschriften
  - IDW Prüfungsstandard zur Prüfung von Softwareprodukten (IDW PS 880)
- Rundschreiben 10/2012 (BA) – Mindestanforderungen an das Risikomanagement (MaRisk) Geschäftszeichen: BA 54-FR 2210-2012/0002 vom 14. Dezember 2012 der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Relevant sind ferner **Beauftragtenthema-spezifische** rechtliche Grundsätze und Richtlinien, u. a.:

- Gefährdungsanalyse und Kontrollplanung Zentrale Stelle
  - § 25h Abs. 4 i.V.m. § 25h Abs. 1 KWG
  - § 9 Abs. 1 und Abs. 2 Nr. 2 GwG
  - BaFin-Rundschreiben 8/2005 (GW) vom 24. März 2005
- Auslegungs- und Anwendungshinweise der Deutschen Kreditwirtschaft zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen“ (DK-Hinweise) MAR kompakt
  - Gesetz über den Wertpapierhandel (WpHG)
  - Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission

Darüber hinaus haben wir im Laufe des Zertifizierungsprozesses und in Zusammenarbeit mit der Wirtschaftsprüfungsgesellschaft auch für künftige Softwareentwicklungen Nutzen ziehen können. Einige positive Aspekte möchten wir nachfolgend darstellen.

Im Rahmen der Zertifizierungen wurden für die zertifizierten Systeme – Gefährdungsanalyse, Kontrollplanung und MAR kompakt – sogenannte **Prozesslandkarten** erstellt, mit deren Hilfe sich die Grundzusammenhänge auf einen Blick erschließen.

Prozesslandkarten enthalten alle relevanten Prozesse und Teilprozesse für die Dienstleistungserbringung. Aus der Prozesslandkarte sind sowohl Prozessbeginn als auch -ende sowie die beteiligten Parteien (Abteilungen der GenoTec/Bank/Beauftragter), die verwendeten Softwarefunktionen und Datenbanken, sämtliche verwendeten Datenquellen sowie die eingebetteten Kontrollen inkl. der IT-Kontrollen (z. B. Eingabe-und Verarbeitungskontrollen) ersichtlich. Es wird erkennbar, wann die Software zum Einsatz kommt, wann Prozessschritte automatisiert und wann manuell durchgeführt werden.

Durch die komprimierte Darstellung wird das Verständnis der Anwendung wesentlich verbessert. Wechselwirkungen, z. B. bei Änderungen in den Schnittstellen, werden einfacher sichtbar. Davon profitieren alle: Beauftragte, Mitarbeiter des IT-Supports oder auch interne und externe Prüfer.

AUTORIN UND ANSPRECHPARTNERIN

Iris Hauptführer
Leiterin Produktentwicklung,
E-Mail: iris.hauptfuehrer@geno-tec.de

Alle zertifizierten Module enthalten selbstverständlich eine Vielzahl notwendiger Validierungen, um Anwendungsfehler (z. B. falsche oder unplausible Eingaben) zu vermeiden. Im Rahmen der Zertifizierung haben wir **Eingabemasken durch Benutzerhinweise und weitere Validierungen verbessert,** um Fehlbedienungen (mögen sie auch nur theoretisch erscheinen) zu vermeiden.

Aber vor der Anwendung und Prüfung einer Software steht deren Entwicklung. Eine Zertifizierung nach PS 880 bedeutet in diesem Zusammenhang erhöhte Anforderungen an die Dokumentation von Anfang an.

Ein wesentlicher Baustein der Zertifizierung waren demnach auch die **Nachvollziehbarkeit der Anforderungen** und die **Umsetzung in der Entwicklung.** Zielsetzung der Prüfung hier: Wurde das Programm auch entsprechend den fachlichen Vorgaben entwickelt (sogenannte Programmidentität)? Für den Entwicklungsprozess ist eine gute Abstimmung zwischen Softwareentwicklung und Produktentwicklung unabdingbar. Die Beteiligten sollten wechselseitig wissen, welchen Zweck die Anwendung abbilden soll, welche Rahmenbedingungen, Restriktionen oder Möglichkeiten in der Softwarearchitektur vorhanden sind.

Über eine Standardisierung wird sichergestellt, dass wesentliche Punkte wie die Beschreibung der Aufgabe (Funktionalität), die Aufgabenträger, die Art der gewünschten Funktionalität (maschinell oder manuell), die Datenquellen, zeitliche und logische Bedingungen und die Verbindlichkeit (muss, soll, kann) nachvollziehbar benannt und dokumentiert sind. Je klarer die Anforderungen sind, umso weniger Missverständnisse entstehen. Unnötiger Entwicklungsaufwand wird reduziert. Eng an den spezifischen Anforderungen können die Testfälle definiert werden. Diese bilden die Basis für die Abnahme und Freigabe der Anwendung durch die Fachabteilung.

Eine sachgerechte Dokumentation ist Voraussetzung für die Nachvollziehbarkeit und damit die Prüfbarkeit des Verfahrens. Umfang und Aussagefähigkeit der Dokumentation einer Software sind somit wichtige Qualitätskriterien für Anwender und Prüfer.

Fazit

Zusammenfassend ist die Zertifizierung sowohl im Innen- als auch im Außenverhältnis eine nutzenstiftende Entscheidung:

- Beauftragte, Analysten und Entwickler (GenoTec-interne Anwender)
  - Erhöhung der Transparenz und der Nachvollziehbarkeit der jeweiligen Anwendung
  - verbesserte Kommunikation zwischen Fachbereich und IT-Entwicklung
  - Qualitätsverbesserung in der Anwendungsentwicklung und den Testverfahren
- interne und externe Prüfungen
  - Bestätigung der Ordnungsmäßigkeit, Funktionsfähigkeit und Sicherheit der Funktionen durch das Testat einer unabhängigen Wirtschaftsprüfungsgesellschaft
  - Verbesserung der Aussagefähigkeit und Nachvollziehbarkeit von Anwender-, Fach- und Systemdokumentationen
  - IT-spezifische Ergänzung der Zertifizierung nach IDW PS 951 Typ 2
- Beauftragte in den Banken (externe Anwender)
  - einheitliche Qualitätsstandards bei der Erbringung der Dienstleistung
  - Vertrauen in die sachgerechte Ausgestaltung der Arbeitsmittel der Beauftragten
  - Sicherheit gegenüber externen Prüfern und der Bankenaufsicht

Für Rückfragen zu den Zertifizierungen nach IDW PS 880 stehen wir Ihnen gerne zur Verfügung.