

VERSTÄNDNISGEWINNUNG

1

Schritt 1
Geschäftstätigkeit; Umfeld; Rechnungslegungsgrundsätze

Allgemeine übergreifende Aspekte

- Verstehen
- Erstwürdigung

Kenntnisse

- Externes Umfeld, einschl. maßgebendes Rechnungslegungssystem
- Merkmale der Einheit, einschl. Rechnungslegungsmethoden
- Ziele, Strategien und rechnungslegungsbezogene Geschäftsrisiken
- Messung und Überwachung des wirtschaftlichen Erfolgs (Kennzahlen)

Zielsetzung

- Verständnis für inhärente Risikofaktoren

Allgemeine übergreifende Kriterien (Auswahl)

- Organisationsstruktur
- Eigentümerschaft
- Führung und Überwachung der Einheit
- Geschäftsmodell
- Integration IT-Einsatz**
- Branchenbezogene, regulatorische und andere externe Faktoren
- Intern und extern genutzte Erfolgskennzahlen
- Maßgebende Rechnungslegungsgrundsätze
- Rechnungslegungsmethoden der Einheiten
- Gründe für etwaige Änderungen

Spezielle Aspekte in Zusammenhang mit Kryptowährungen:

Verstehen, **wie** Kryptowährungen bei der Unternehmung

- erworben** (Mining, Erwerb über Börse gegen Euro, Tausch gegen Produkte/Dienstleistungen etc),
- verwaltet** (eigene Wallets, Drittverwahrer..) und
- verwendet** (Nutzungszweck der Kryptowährung als
 - Zahlungsmittel
 - Investition/Wertanlage
 - Sonstiges)

werden.

Verstehen **des IT-Einsatzes für Kryptowährungen:**

- Identifikation der **eingesetzten Wallets und deren Anbieter**
 - Zugang, Schnittstellen,
 - Automatisierter Datenaustausch von Börse/Wallet-System und ERP-System
- Identifikation der **eingesetzten Software**
 - für Krypto-Transaktionsverwaltung** im Unternehmen und
 - für deren **Buchhaltung**

2

Schritt 2
Prüfungsbezogenes internes Kontrollsystem (IKS)

Allgemeine übergreifende Aspekte:

- Sichtung
- Schaffung eines Mindestverständnisses
- Kenntniserwerb Kontrollaktivitäten

Kenntnisse

Vorrangig: Gewinnung Verständnis Komponenten 1-4

- Kontrollumfeld
- Risikobeurteilungsprozess
- Rechnungslegungsrelevantes Informationssystem
- Überwachung des IKS

Beurteilung: Aufbau und Implementierung der

- Kontrollaktivitäten

Zielsetzung

- Mindestverständnis

Spezielle Aspekte in Zusammenhang mit Kryptowährungen:

Verständnis Kontrollen innerhalb IT-Systeme:

- Zugriffs- und Berechtigungskonzepte**
 - Wer hat Zugang zu den Wallets und den privaten Schlüsseln?
 - Wie ist der Zugriff geregelt, dokumentiert beschränkt?
 - Nutzung von Multi-Signature-Verfahren?
- Back-up- und Recovery-Prozesse**
 - Wie werden Wallet-Daten, insbesondere private Keys, gesichert?
 - Was passiert bei Verlust der Zugriffsdaten?
- Sicherheitskonzepte und Schutzmaßnahmen gegen Cyber Risiken**
 - Einsatz von Firewalls, Virensclannern, Zwei-Faktor-Authentifizierung
 - Regelmäßige Sicherheitsupdates und
 - Penetrationstests

Verständnis der Transaktionsprozesse:

- Abläufe bei Erwerb, Verkauf und Tausch von Kryptowährungen**
 - Wer initiiert Transaktionen?
 - Wie erfolgt die Autorisierung und Dokumentation?
- Verwendung im Unternehmen**

Sind Kryptowährungen separat oder in operative Prozesse integriert?

Schnittstellen zu weiteren Systemen

- Integration in ERP-Systeme und Buchhaltung**
 - manuelle oder automatisierte Buchungen?
 - Nachvollziehbarkeit der Abstimmung der Daten zwischen Wallets und Buchhaltung?
- Datenaufbereitung und Nachvollziehbarkeit**
 - Dokumentation von Transaktionen (z. B. Hashes, Zeitstempel, Gegenpartei)
 - Nutzung von Blockchain-Explorern zur Nachverfolgung?

Stand: 01.10.2025

RISIKOIDENTIFIZIERUNG

3

Schritt 3
Identifizierung Risiken auf Abschlussebene

Einfluss von Faktoren auf den Abschluss als Ganzes oder auf eine Vielzahl von Aussagen

- Indikatoren Integrität Management
- Geschäftsgebaren
- Branche
- Insolvenznähe, Going-Concern?

Spezielle Aspekte für Kryptowährungen:

Kryptowährungen sind anonymisierbar, schnell übertragbar und schwer kontrollierbar.

Risiken für Fraud:

Im Extremfall ermöglichen sie dem Management:

- Verschleierung von Vermögenswerten** (z.B. Nutzung nicht offengelegter Wallets)
- Nicht deklarierte Transaktionen** mit nahestehenden Personen oder Dritten
- Bilanzfälschung** durch falsche Angaben zu Bestand, Bewertung oder Eigentum

Going-Concern-Risiken:

Wenn das Unternehmen **sehr stark auf Kryptowährungen setzt**, könnte aufgrund der **Volatilität** die Unternehmensfortführung bei **Totalverlust** gefährdet werden.

4

Schritt 4
Relevante Aussagen / Verstehen inhärenter Risikofaktoren / Wesentliche Kategorien von Geschäftsvorfällen sowie relevante Kontrollen

Risikobeurteilung nach ISA [DE] 315 (Revised 2019): „Spektrum der inhärenten Risiken“ (Aspekte, die bei Kryptowährungen in die Risikoidentifikation einbezogen werden könnten)									
Relevante Risiken auf Aussageebene		GuV-Posten / Bilanz-Posten / Anhangangaben							
z. B. Kryptowährungen (Sonstige Vermögensgegenstände)		E	R&V	V	B	A	R	P	G
		Existenz	Eigentum	Vollständigkeit	Bewertung	Ausweis	Rechnerische Richtigkeit	Abgrenzung	Genauigkeit
Inhärente Risikofaktoren	1 Komplexität	Verifizierung über Blockchain erfordert technisches Know-how	Verwaltung privater Schlüssel und Multi-Signatur-Wallets erhöht Komplexität	Fragmentierte Transaktionshistorie über verschiedene Börsen/Blockchains	Unterschiedliche Bewertungsmethoden (Börsenkurs vs. Interne Modelle)	Unsicherheit bei Klassifikation (Umlauf- oder Anlagevermögen)	Manuelle Übertragung von Blockchain-Daten in Fibu	Zeitliche Zuordnung bei Übertragung von Währungen auf verschiedene Blockchains	Unterschiedliche Dezimalstellen bei Token (z.B. ETH 18, BTC: 8)
	2 Subjektivität	Abhängigkeit von externen Blockchain-Explorern oder Wallet-Anbietern	Zugehörigkeit Wallets zum Unternehmen objektiv belegbar	Subjektive Erfassung von Transaktionen aus dezentralen Quellen	Subjektive Auswahl relevanter Marktdaten	Ausweisentscheidung bei hybrider Nutzung (Zahlungsmittel/ Investition)	Subjektive Interpretation von Transaktionsgebühren	Periodengerechte Erfassung	Schätzung von nicht börsengehandelte n Beträgen
	3 Unsicherheit	Risiko von 51%-Angriffen auf Blockchain	Unklare Rechtslage bei Verlust privater Keys	Evtl. unvollständige Transaktionsprotokolle bei privaten Blockchains	Externe Preisvolatilität	Fehlende gesetzliche Vorgaben	Fehler in Smart Contracts beeinträchtigen Berechnungen	Zeitunterschiede zwischen Blockchain-Bestätigung und Fibu-Buchung	Volatilitätsbedingte Rundungsdifferenzen
	4 Änderungen	Software-Updates können Zugriff auf Wallets beeinträchtigen	Änderungen in Schlüsselverwaltungsprozessen	Neue Transaktionsprotokolle	Regulatorische Änderungen beeinflussen Marktbewertungen	Neue Accounting-Standards	Änderungen in Blockchain-Protokollen	Wechsel Bilanzierungsmethode (FIFO)	Anpassung Bewertungsmodelle bei neuen Vorgaben
	5 Einseitige Ausrichtung / dolose Handlungen	Gefälschte Transaktionsbestätigungen	Diebstahl privater Schlüssel durch Insider	Verschleierung von Transaktionen	Kursmanipulation	Falsche Klassifikation	Verwendung falscher Umrechnungskurse	Vorverlegung Buchungszeitpunkt	Falsche Angaben zum Marktwert
Risikobeurteilung insgesamt (Begründung der Risikobeurteilung)									
Risiko, dass aussagebezogene PH alleine nicht ausreichend sind (nur im Falle einer Feststellung zu dokumentieren)									

Bedeutsame Risiken ?