[Logo der Organisation]

[Name der Organisation]

VERFAHREN FÜR INTERNE AUDITS

Code:	
Version:	
Datum der Version:	
Erstellt durch:	
Genehmigt durch:	
Vertraulichkeitsstufe:	

Commented [27A1]: Um zu erlernen, wie Sie dieses Dokument ausfüllen und echte Beispiele darüber zu sehen, was Sie schreiben müssen, schauen Sie sich dieses Video-Tutorial an:
"How to Write ISO 27001/ISO 22301 Internal Audit Procedure and Audit Program".

Um auf das Tutorial zuzugreifen: Suchen Sie in Ihrem Posteingang die E-Mail, die Sie zum Zeitpunkt des Kaufes erhalten haben. Dort finden Sie einen Link und ein Passwort, mit denen Sie auf das Video-Tutorial zugreifen können.

Commented [27A2]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

Commented [27A3]: Um mehr zu diesem Thema zu erfahren:

- lesen Sie diesen Artikel: Probleme bei internen Auditoren nach ISO 27001 und BS 25999-2 https://advisera.com/27001academy/de/blog/2011/03/25/probleme-bei-internen-auditoren-nach-iso-27001-und-bs-25999-2/
- nehmen Sie an diesem kostenlosen Online-Training teil: ISO 27001:2013 Internal Auditor Course https://training.advisera.com/course/iso-27001-internal-auditor-course/
- schauen Sie sich dieses Buch an: ISO Internal Audit: A Plain English Guide https://advisera.com/books/iso-internal-audit-plain-english-guide/

Commented [27A4]: Die Systematik für die Kodierung von Dokumenten sollte dem in der Organisation vorhandenen System zur Dokumentations-Kodierung entsprechen. Falls kein solches System vorhanden ist, kann diese Zeile gelöscht werden.

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
	0.1	27001Academy	Erster Entwurf des Dokuments

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Verfahrens ist die Beschreibung aller Aktivitäten in Zusammenhang mit Audits – Erstellung des Audit-Programms, Auswahl eines Auditors, Durchführung individueller Audits und Berichterstattung.

Dieses Verfahren wird auf alle Aktivitäten angewendet, die innerhalb des Informationssicherheits-Managementsystems (ISMS) [Betrieblichen Kontinuitätsmanagementsystems (BKMS)] durchgeführt werden.

Anwender dieses Dokuments sind [Mitglieder der Unternehmensführung] von [Name der Organisation], sowie interne Auditoren.

Commented [27A5]: Dies ist statt ISMS einzusetzen, falls sich das Verfahren ausschließlich auf betriebliches Kontinuitätsmanagement bezieht.

Commented [27A6]: Das Führungsgremium innerhalb des ISMS/BKMS Anwendungsbereiches.

Commented [27A7]: Geben Sie bitte den Namen Ihrer Organisation an.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitt 9.2
- ISO 22301 Norm, Abschnitt 9.2
- Informationssicherheitspolitik
- Richtlinie für betriebliches Kontinuitätsmanagement
- Verfahren zu Korrekturmaßnahmen

Commented [27A8]: Löschen, falls sich das Verfahren ausschließlich auf betriebliches Kontinuitätsmanagement bezieht.

Commented [27A9]: Löschen, falls sich das Verfahren ausschließlich auf Informationssicherheit bezieht.

Commented [27A10]: Löschen, falls sich das Verfahren ausschließlich auf betriebliches Kontinuitätsmanagement bezieht.

3. Internes Audit

3.1. Zweck des internen Audits

[redacted]

entsprechen. Ebenso ob sie wirksam umgesetzt und aufrechterhalten werden und ob sie die Anforderungen der Richtlinien und die Zielsetzungen erfüllen.

Commented [27A11]: Löschen, falls sich das Verfahren ausschließlich auf betriebliches Kontinuitätsmanagement bezieht.

Commented [27A12]: Löschen, falls betriebliches Kontinuitätsmanagement nicht umgesetzt wird.

[redacted]

Commented [27A13]: Löschen Sie diesen Absatz, wenn der Interne Auditor diese Aufgabe nicht ausführt.

3.2. Planung interner Audits

[Stellenbezeichnung] genehmigt ein Internes Audit-Programm, das wie in Anhang 1 umrissen erstellt wird.

Commented [27A14]: Zum Beispiel: Manager der betrieblichen Kontinuität, Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter usw.

Eines oder mehrere Audits sollten während eines [redacted]

Das Interne Audit-Programm muss folgende Informationen zu jedem einzelnen Audit enthalten:

- Zeitspanne des Audits (Angabe von Start- und End-Datum oder Monat in dem das Audit geplant ist)
- [illegible]
- [illegible]
- [illegible]
- Wer das Audit durchführt (falls es mehr als ein Auditor ist, den Leiter des Audit-Teams angeben)

Durchgeführte Audits müssen im Internen Audit-Programm protokolliert werden.

3.3. Ernennung von internen Auditoren

[Stellenbezeichnung] soll interne Auditoren ernennen.

Commented [27A15]: Zum Beispiel: Manager der betrieblichen Kontinuität, Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter usw.

Ein interner Auditor kann jemand aus [illegible] :

- Kenntnis der ISO/IEC 27001 und ISO 22301 Normen
- [illegible]
- [illegible]

Commented [27A16]: Löschen, falls sich das Verfahren ausschließlich auf betriebliches Kontinuitätsmanagement bezieht.

Commented [27A17]: Löschen, falls betriebliches Kontinuitätsmanagement nicht umgesetzt wird.

[illegible] d.h. es müssen Interessenskonflikte vermieden werden, da Auditoren ihren eigenen Arbeitsbereich nicht prüfen dürfen.

[illegible]

Commented [27A18]: Oder ISO 22301

3.4. Durchführung individueller interner Audits

Commented [27A19]: Lesen Sie diesen Artikel für Tipps zur Durchführung effektiver Audits:

7 ways to improve the internal audits of your ISO 27001 ISMS https://advisera.com/27001academy/blog/2017/08/28/7-ways-to-improve-the-internal-audits-of-your-iso-27001-isms/

Für individuelle interne Audits verantwortliche Personen sind im Jahresprogramm für interne Audits genannt. [illegible]

Folgendes muss während eines internen Audits berücksichtigt werden:

- Die im Internen Audit-Programm festgelegten Kriterien
- [illegible]
- [illegible]
- [illegible]

Folgende Ergebnisse eines internen Audits müssen aufgezeichnet werden:

- [redacted]
- [redacted]

Commented [27A20]: Z.B. Manager der betrieblichen Kontinuität, Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter, Verantwortlicher für den Geschäftsbereich usw.

4. Verwaltung von Aufzeichnungen zu diesem Dokument

Name der Aufzeichnung	Aufbewahrungs-Ort	Verantwortlicher für Aufbewahrung	Maßnahme zum Schutz der Aufzeichnung	Aufbewahrungs-Dauer
Internes Audit-Programm (in elektronischer Form)	Rechner von [Stellen-bezeichnung]	[Stellenbezeichnung]	Nur[Stellenbezeichnung] und der interne Auditor haben die Berechtigung für das Erstellen von Einträgen oder für Änderungen am Jährlichen Programm für interne Audits.	Programme werden für die Dauer von 3 Jahren aufbewahrt
Interner Audit-Bericht (in elektronischer Form)	Rechner des internen Auditors und von [Stellen-bezeichnung]	Interner Auditor	Berichte werden schreibgeschützt gespeichert	Berichte werden für die Dauer von 3 Jahren aufbewahrt
Interne Audit-Checkliste (das während des internen Audits ausgefüllte Formular)	Rechner des internen Auditors	Interner Auditor	Die Checkliste wird schreibgeschützt gespeichert	Die Checkliste wird für die Dauer von 3 Jahren aufbewahrt

Commented [27A21]: Passen Sie den Zeitraum in dieser Spalte Ihren spezifischen Bedürfnissen an.

Commented [27A22]: Üblicherweise die Person, die das Interne Audit-Programm genehmigt hat.

Commented [27A23]: Üblicherweise in PDF-Format.

Commented [27A24]: Üblicherweise in PDF-Format.

[redacted]

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

Der Eigentümer des Dokuments ist [Stellenbezeichnung], der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Commented [27A25]: Zum Beispiel: Manager der betrieblichen Kontinuität, Sicherheitsmanager, Informationssicherheitsmanager, Compliance-Beauftragter usw.

Commented [27A26]: Dies ist nur eine Empfehlung; nach Bedarf anpassen.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- [illegible]
- [illegible]
- [illegible]

6. Anhänge

- Anhang 1 – Internes Audit-Programm
- Anhang 2 – Interner Audit-Bericht
- Anhang 3 – Interne Audit-Checkliste

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A27]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.