Freistaat Thüringen
Thüringer Landesrechenzentrum

Informationssicherheitsmanagement des TLRZ

Richtlinie zur internen ISMS-Auditierung

Version / Datum	6.1	31.05.2021
Dateiname	1040.ISMS.RL_Interne Audits.Docx	
Dokumententyp	Richtlinie	
Vertraulichkeitsstufe	**TLP GREEN**	
Verantwortlicher	ISB TLRZ	
Erstellt am	19.02.2020	
Status	**freigegeben**	
Verteiler	ISM-Team CNFT, ISM-Team Land, ISB Land, ISB-Ressorts	
Dokumentenablage	VIS: 25.10-1073-15833/2021	
Ersteller (Name/Rolle)	TLRZ Weide, Günter	

TLP:GREEN: Organisationsübergreifende Weitergabe
Informationen dieser Stufe dürfen innerhalb der Organisationen und anderen Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

Dokumentenfreigabe:

- keine erneute Freigabe erforderlich -

Inhaltsverzeichnis

1 Allgemeines

1.1 Zielsetzung

Diese Richtlinie definiert den Rahmen für die interne Auditierung des Informationssicherheits-Managementsystems (ISMS), welches nach den Grundsätzen der Leitlinie zur Informationssicherheit [1]. aufgebaut und kontinuierlich als IT Sicherheitsprozess implementiert wurde.

1.2 Geltungsbereich

Das vorliegende Dokument gilt für alle IT-Systeme die vom TLRZ gemangt, bereitgestellt und/ oder betrieben werden. Darüber hinaus gilt es explizit für den Informationsverbund „Corporate Network Freistaat Thüringen" (CNFT)“
Den Behörden und Einrichtungen der Thüringer Landesverwaltung wird die sinngemäße Anwendung empfohlen, wenn keine eigenen Regelungen getroffen wurden.

1.3 Geltungsdauer/ Revision

Die Geltungsdauer dieses Dokuments ist nicht befristet.
Das vorliegende Dokument wird entweder anlassbezogen oder mindestens alle 2 Jahre einer überprüfenden Fortschreibung unterzogen. Das Dokument wird dabei, nach dem KVP durch Mitglieder des ISM-Teams des- Informationsverbundes inhaltlich überprüft und im Bedarfsfall fortgeschrieben. Dieses Dokument unterliegt der Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen [2].

2 Goldene Regeln

Die folgenden Regeln gelten als die Elementaren Anforderungen und sollen einen schnellen ersten Überblick geben.

- Es muss ein Verantwortlicher für interne Audits festgelegt werden.
- Für interne Audits und Revision der Anschlussbedingungen, muss ein Prüfplan mit einen Jahr Vorausplanung erstellt werden.
- Das Audit- oder Revisionsteam darf nicht aus Mitarbeitern des zu prüfenden Bereiches bestehen.
- Ergebnisse des internen Audits müssen schriftlich und nachweisbar festgehalten werden und in Form eines Managementberichts der Leitung vorgelegt werden.
- Ergebnisse einer Revision der Anschlussbedingungen müssen schriftlich und nachweisbar festgehalten werden und werden dem ISB-Land für ein abschließendes Votum und dem zuständigen Ministerium der geprüften Behörde vorgelegt.
- Vor einer Auditierung oder Revision, muss diese Schriftlich angekündigt werden.
- Für festgestellte Abweichungen, von den Anforderungen vom IT-Grundschutz des BSI, müssen Fristen für eine Behebung der Abweichungen festgelegt werden.
- Das Audit- und Revisionsteam muss entsprechende Qualifikation aufweisen können

3 Einleitung

Die Wirksamkeit und Handlungsfähigkeit von Behörden und Einrichtungen in der Landesverwaltung ist in hohem Maße von der Funktionsfähigkeit der Informationstechnik abhängig. Die Gewährleistung der Funktionsfähigkeit erfolgt über interne Audits und durch Revision der Anschlussbedingungen. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheitsprozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden.
Durch die IT-Grundschutz-Audits wird die Umsetzung der verschiedenen Anforderungen des IT-Grundschutzes innerhalb eines Informationsverbundes überprüft. Dies wird von BSI-zertifizierten Auditoren durchgeführt, um hier eine gleichbleibend hohe Qualität der Audits zu gewährleisten. Die Audits sind notwendig, um verschiedene Zertifikate zu erlangen, wie beispielsweise das ISO 27001 Zertifikat auf Basis von IT-Grundschutz.
Im Gegensatz dazu werden im Informationsverbund CNFT interne Audits durchgeführt, um die Qualität der Umsetzung von anforderungsgerechten Maßnahmen des IT-Grundschutzes zu gewährleisten. Dabei werden einzelne im Informationsverbund modellierte Bausteine und Maßnahmen aus dem IT-Grundschutz des BSI nach vorher festgelegten Prüfkriterien an einzelnen Standorten des Informationsverbundes durch qualifizierte Auditoren unabhängig überprüft und dokumentiert.
Die Revision der Anschlussbedingungen dient der überblicksmäßigen Prüfung der Umsetzung der Sicherheitsmaßnahmen, die unabdingbare Voraussetzungen für den Anschluss an das Landesdatennetz sind. Diese Grundlagenprüfung ist Bestandteil eines erfolgreichen Informationssicherheitsmanagements und erfolgt durch fachlich qualifizierte sowie zweckbezogen ausgebildete und extern zertifizierte Bedienstete des Freistaats Thüringen (IS-Revisoren).

4 Interne Audits (iA)

4.1 Definition interne Audits

Unter internen Audits versteht man eine umfassende Überprüfung der ordnungsgemäßen Umsetzung des, für den Informationsverbund festgelegten, Sicherheitsprozesses. Diese Überprüfung erfolgt auf Grundlage im Vorfeld festzulegenden Prüfkriterien, der für den Informationsverbund anzuwendenden IT-Grundschutz-Maßnahmen, durch fachlich qualifizierte Mitarbeiter. Im Rahmen des internen Audits erfolgt keine Beratung der zu prüfenden Behörde oder Einrichtung.

4.2 Ziele von internen Audits

Das Ziel von internen Audits besteht darin, die in den IT-Grundschutzaudits geforderten Maßnahmenumsetzungen des IT-Grundschutzes des BSI in einem vorher festgelegten Prüfungsumfang in ausgewählten Bereichen, Dienststellen oder Standorten des Informationsverbundes CNFT durch fachlich qualifizierte Auditoren unabhängig zu überprüfen und zu dokumentieren.

4.3 Verantwortlichkeiten für interne Audits

Festlegung 1	Die Wahrung der Gesamtverantwortung für interne Audits trägt die Leitungsebene des TLRZ.

Festlegung 2	Die Leitungsebene muss regelmäßig über Probleme, Ergebnisse und Aktivitäten der internen Audits, aber auch über neue Entwicklungen, geänderte Rahmenbedingungen oder Verbesserungsmöglichkeiten informiert werden.

4.3.1 Die Verantwortung für interne Audits

Festlegung 3	Die Aufgabe des Verantwortlichen für interne Audits im TLRZ wird von RL25 wahrgenommen.

Zu den Aufgaben des Verantwortlichen gehören:

- Sicherstellung, dass die Ergebnisse des Audits dazu verwendet werden, um die Sicherheitsmaßnahmen zu verbessern
- Erstellung eines Auditplanes
- Festlegung von Ziele des internen Audits, zusammen mit dem ISB des Informationsverbundes
- Vorlage eines jährlichen Managementberichts an die Leitungsebene

- Schriftliche Information der von dem jeweiligen internen Audit betroffenen Bereiche bzw. Themenverantwortlichen

Festlegung 4	Alle Organisationseinheiten im Informationsverbund müssen den Verantwortlichen für interne Audits in seiner Aufgabenwahrnehmung unterstützen.

4.3.2 Das interne Auditteam

Festlegung 5	Das interne Auditteam übernimmt die konkrete Durchführung der internen Audits im jeweiligen Informationsverbund.

Zur Erfüllung der Aufgabe wird diesen ein uneingeschränktes aktives und passives Informationsrecht während der jeweiligen Prüfung gewährt. Dazu gehört auch das Recht auf Einsichtnahme in vertrauliche Unterlagen bzw. Daten, soweit dies für die jeweilige Prüfung erforderlich ist. Falls es sich bei den einzusehenden Daten um VS-Unterlagen handelt, so müssen die entsprechenden gesetzlichen Regelungen und Verordnungen dazu eingehalten werden.

Festlegung 6	Bei der Wahrnehmung der Prüfaufgaben müssen vom internen Auditteam folgende Revisionsprinzipien eingehalten werden: • Rechtschaffenheit und Vertraulichkeit • Fachkompetenz • Objektivität und Sorgfalt • Sachliche Darstellung der Prüfergebnisse • Nachweise über Prüfergebnisse und Nachvollziehbarkeit

Festlegung 7	Das eingesetzte interne Auditteam muss zur Gewährleistung der Unabhängigkeit und Objektivität mindestens aus 2 Auditoren (4-Augen-Prinzip) bestehen.

Festlegung 8	Es sollte sichergestellt sein, dass der laufende Betrieb im jeweiligen Informationsverbund durch die internen Audits nicht wesentlich behindert wird.

4.3.3 Pflichten aller Mitarbeiter

Festlegung 9	Alle Mitarbeiter im jeweiligen Informationsverbund sind verpflichtet, die Arbeit der internen Auditoren zu unterstützen und zu fördern. Alle Mitarbeiter

	müssen den internen Auditoren die notwendigen Auskünfte wahrheitsgemäß und vollständig erstatten, sowie die erforderlichen Unterlagen und Daten überlassen.

4.4 Planung von internen Audits

Der Umfang der internen Audits wird mindestens jährlich im Voraus geplant. Im Informationsverbund CNFT erfolgt dies durch den Auftragnehmer des Los 7 (IABG GmbH) in Zusammenarbeit mit dem ISB. Die Planung soll die Benennung der einer näheren Prüfung zu unterziehenden Bausteine oder Maßnahmen des IT-Grundschutzes und die zum Audit vorgesehenen Standorte umfassen. Die Auditplanung ist als Anlage zu dieser Richtlinie zu dokumentieren.

4.5 Durchführung von internen Audits

Festlegung 10	Interne Audits werden grundsätzlich von Mitgliedern des CERT vorgenommen.

Festlegung 11	Abweichend von Festlegung 10, werden die internen Audits im Informationsverbund CNFT von einem internen Auditteam des Auftragnehmers des Los 7 (IABG mbH) unabhängig durchgeführt.

Um die Unabhängigkeit zu gewährleisten, führen die Mitarbeiter des ISM-Team CNFT keine internen Audits im Informationsverbund CNFT durch

Festlegung 12	Für eine Durchführung von internen Audits muss das Auditteam vom Verantwortlichen für interne Audits schriftlich beauftragt werden.

Festlegung 13	Die Beauftragung muss alle für die Prüfungsdurchführung gemäß interner Auditplanung erforderlichen Informationen (Prüfungsgegenstand, Prüfmethoden, Haftung) enthalten.

Festlegung 14	Die vom Audit betroffenen Bereiche bzw. Themenverantwortlichen müssen schriftlich durch den Verantwortlichen für interne Audits informiert werden.

Das Informationsschreiben sollte den Auditgegenstand, Auditzeitraum und die Namen des internen Auditteams beinhalten.

Festlegung 15	Bei der Durchführung sollte darauf geachtet werden, dass die gewählten Prüfmethoden verhältnismäßig sind.

4.6 Ergebnisse der internen Audits

Festlegung 16	Die Ergebnisse der internen Audits müssen dokumentiert und durch das ISM-Team und den ISB des Informationsverbundes ausgewertet werden.

Festlegung 17	Für im Audit festgestellte Abweichungen von den Vorgaben des IT-Grundschutzes des BSI[1], muss eine Frist zur Nachbesserung und Abstellen der Abweichung festgelegt werden.

Die Resultate der internen Audits sind Teil des Managementberichts, welchen dem Leiter Organisation, durch den Verantwortlichen für interne Audits vorgelegt wird.

4.7 Auswertung und Nachkontrolle der Auditergebnisse

Festlegung 18	Die Ergebnisse eines durchgeführten internen Audits müssen durch den Verantwortlichen für interne Audits zusammengefasst und der Leitungsebene in angemessener Form präsentiert werden.

Festlegung 19	Auf Basis des internen Auditberichtes muss die weitere Auditplanung geprüft und ggf. angepasst werden

Vor Fertigstellung des jeweiligen Auditberichtes werden die festgestellten Abweichungen mit dem jeweiligen Themenverantwortlichen besprochen und abgestimmt. Ziel dieser Abstimmung ist es, mögliche Unstimmigkeiten über die jeweilig festgestellten Abweichungen zu vermeiden.

Festlegung 20	Nach der Abstimmung ergeben sich folgende 2 Möglichkeiten für Abweichungen: • Abweichung Klasse 1: Es besteht **Einigkeit** über die **Existenz** der festgestellten Abweichung zwischen dem Themenverantwortlichen und dem internen Auditteam. • Abweichung Klasse 2:

[1] [3] BSI IT-Grundschutz Standard
Dokument:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

	Es besteht **keine Einigkeit** über die **Existenz** der festgestellten Abweichung zwischen dem Themenverantwortlichen und dem internen Auditteam.

Die Abweichungsklassen müssen im Auditbericht mit angegeben werden.

Festlegung 21	Aus den Prüfergebnis resultierende Aufgaben, werden durch den Verantwortlichen für interne Audits und den jeweiligen Themenverantwortlichen wahrgenommen.

Festlegung 22	Die festgestellten Sicherheitsmängel müssen an die jeweiligen Themenverantwortlichen zur Stellungnahme weitergeleitet werden. Für eine Stellungnahme, zu den identifizierten Mängeln, von den jeweiligen Themenverantwortlichen besteht eine Frist von 4 Wochen.

Hierbei ist zu beachten, dass nur die für den jeweiligen Bereich notwendigen Informationen zur Verfügung gestellt werden („Need to know"-Prinzip). Die Stellungnahme sollte erste Lösungsansätze und Einschätzungen zu Aufwänden und Fertigstellungstermine für diese darlegen.

Festlegung 23	Der Verantwortliche für interne Audits muss über die geplante Mängelbehebung und über Erfolg und Misserfolg dieser, informiert werden.

Festlegung 24	Für die Umsetzung der Verbesserungen sind die betroffenen Bereiche sowie der jeweilige Themenverantwortliche verantwortlich.

Festlegung 25	Nicht-Einhaltung von gesetzten und abgestimmten Terminen zur Beseitigung von Mängeln sind vom jeweiligen Themenverantwortlichen unverzüglich dem Verantwortlichen für interne Audits zu melden, wenn die Informationssicherheit im jeweiligen Informationsverbund durch die Mängel erheblich gefährdet ist.

Festlegung 26	Der Verantwortliche für interne Audits muss zur Nachverfolgung über die, bei den internen Audits, identifizierten Sicherheitsmängel und Handlungsempfehlungen eine offene Punkte-Liste (OPL)führen und diese aktuell halten.

5 Revision der Anschlussbedingungen (RdAB)

5.1 Definition Revision

Unter einer IS-Revision der Anschlussbedingungen CNFT versteht man die Überprüfung des Umsetzungsstandes der Anschlussbedingungen der an den Informationsverbund angeschlossenen Dienststelle oder Standorte. Dies geschieht auf der Grundlage der Mindestanforderungen der Anschlussbedingungen und der zugrundeliegenden IT-Grundschutz Bausteine. Eine Revision enthält neben der Prüfung der Anforderungen eine Beratung bzw. eine Empfehlung zur weiteren Vorgehensweise.

5.2 Ziele der Revision

Das Ziel der Revision der Anschlussbedingungen ist es, die Einhaltung der Anschlussbedingungen des Informationsverbunds CNFT in den Standorten zu dokumentieren und Hinweise zur Verbesserung des Sicherheitsstatus zu erteilen.

5.3 Planung der Revision

Festlegung 27	Für den Informationsverbund sollen ca. dreißig ausgewählte Dienststellen oder Standorte im Jahr, maximal jedoch 10 Prozent der bereits an den Informationsverbund angeschlossenen Behörden oder Einrichtungen überprüft werden.

Dabei soll ein Querschnitt aus verschiedenen Geschäftsbereichen und Aufgaben der Landesverwaltung betrachtet werden. Die im jeweils nächsten Jahr zu prüfenden Behörden oder Einrichtungen des Informationsverbundes sollen im vierten Quartal des Vorjahres vom ISB-Land gemeinsam mit dem ISM-Team des Landes und des Informationsverbundes ausgewählt werden.

Festlegung 28	Der Prüfplan muss vom CIO des Freistaats Thüringen erlassen werden.

Festlegung 29	Für die Durchführung der Revisionen müssen im ISM Team des Landes angemessene Prüfkataloge abgestimmt werden, die durch die zu prüfenden Dienststellen beantwortet werden muss. Der Prüfkatalog wird ausgefüllt vor der Vor-Ort Prüfung an den Revisor übergeben.

Festlegung 30	Es sollten Revisionslisten geführt werden, die den aktuellen Stand der Revisionsobjekte sowie die geplanten Revisionen dokumentieren.

5.4 Umfang der Revision

Festlegung 31	Die Revision der Anschlussbedingungen erfolgt anhand des Prüfkataloges in Abhängigkeit von der Größe der Dienststelle.

Festlegung 32	Die Prüfung erfolgt durch Plausibilität der Umsetzung auf Maßnahmenebene.

5.5 Durchführung der Revision

Festlegung 33	Die für eine Revision der Anschlussbedingungen ausgewählte Dienststelle oder Standort des Informationsverbundes muss sechs Wochen vor Beginn der Prüfung über den Zeitpunkt, den Umfang und das Revisionsteam unterrichtet werden.

Festlegung 34	Die Revision der Anschlussbedingungen im Informationsverbund CNFT sollen von Mitarbeitern des Freistaats unabhängig durchgeführt werden.

Dies wird sichergestellt, dadurch, dass die prüfenden Mitarbeiter nicht dem Geschäftsbereich der für die Revision ausgewählten Dienststelle zugeordnet sein dürfen.

Festlegung 35	Die Revision soll von zertifizierten internen Revisoren für Informationssicherheit oder Mitarbeitern mit vergleichbarer Ausbildung durchgeführt werden.

Festlegung 36	Zu Beginn der Vor-Ort-Prüfung sollte das Auditteam ein Eröffnungsgespräch mit den Verantwortlichen der betreffenden Institution führen. Danach sollten alle im Prüfplan festgelegten Anforderungen mit den vorgesehenen Prüfmethoden kontrolliert werden.

Innerhalb der Revision werden bei der Vorort-Prüfung die Anschlussbedingungen mittels eines Interviews sowie einer Vorort-Begehung überprüft.

5.6 Ergebnisse der Revision

Festlegung 37	Auf der Basis der bei der Revision der Anschlussbedingungen erfassten Informationen muss vom Revisionsteam ein Revisionsbericht erstellt werden.

Die geprüfte Dienststelle soll hierzu Stellung nehmen können

Festlegung 38	Auf Grundlage des abgestimmten Prüfberichtes, hat der ISB-Land das abschließende Votum.

Das für die geprüfte Dienststelle zuständige Ministerium sowie der Leiter der geprüften Behörde erhalten den Abschlussbericht mit Votum und ggf. Auflagen zugesandt. Das Ergebnis der Revision wird im Managementbericht aufgenommen.

6 Außerplanmäßige interne Audits / Revision der Anschlussbedingungen

Infolge von Sicherheitsvorfällen oder anderen Ereignissen die den IT-Sicherheitsprozess beeinflussen können, kann es erforderlich sein, die betroffenen Bereiche des Informationsverbundes außerplanmäßig zu prüfen.
Gegebenenfalls müssen die für eine außerplanmäßige Prüfung erforderlichen personellen und materiellen Ressourcen kurzfristig bereitgestellt werden. Dazu kann u. U. eine Entscheidung der Leitung des Informationsverbundes notwendig sein, wenn die Kompetenzen der Mitglieder des ISM-Teams für eine solche Entscheidung nicht ausreichen oder aus anderen Gründen im ISM-Team keine Entscheidung über die Bereitstellung der Ressourcen für die außerplanmäßige IS-Revision getroffen werden kann.

7 Ausnahmeregelung

Eine Abweichung von den vorgenannten Festlegungen ist in der Dokumentation des entsprechenden Veränderungsvorgangs (Change) zu begründen, vom zuständigen Informationssicherheitsbeauftragten zu befürworten und vom zuständigen Vorgesetzten gemäß CAB zu genehmigen.

8 Freigaberegelung

Das vorliegende Dokument tritt am Tag nach der Bekanntgabe/Veröffentlichung in Kraft.

9 Mitgeltende Unterlagen

[1] Leitlinie zur Informationssicherheit
Dokument: 1010.ISMS.RL_Leitlinie_Informationssicherheit

[2] Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
Dokument: 1030.ISMS.RL_Dokumentenlenkung

[3] BSI IT-Grundschutz Standard
Dokument:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

10 Änderungsverzeichnis

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
31.05.2021	6.1		Review, redaktionelle Überarbeitung, keine erneute Freigab erforderlich	G. Weide
05.10.2020	6	Freigabe	Konkretisierung in Kap.5.5. dass die Revisoren aus einem anderen Geschäftsbereich kommen	St. Sperling
23.07.2020	5.3	Alle	Änderung des Layouts und der Vorlage; Redaktionelle Überarbeitung; Review gegen Baustein DER.3.1	D. Wittmann
24.01.2020	5.2	3.3, 3.5, 3.7	3.3 Beschreibung der Verantwortlichkeiten für Interne Audits, 3.5 Auditbeauftragung und Ankündigung, 3.7 Auswertung und Nachkontrolle der Auditergebnisse	D. Tribess
13.06.2019	5.1	4.1	Prüfung auf AS-001 Auditbericht. Name IVB korrigiert.	G. Weide
26.02.2019	5		Freigabe	St. Sperling
19.02.2019	4.03	3, 7	Fehlerkorrekturen	G. Weide
12.02.2019	4.02	8	Mitgeltende Dokumente	K. Mühlstein
25.01.2019	4.01	2, 3	Detaillierung Auditteam	D. Tribess
10.10.2018	4.0		Freigabe	St. Sperling
30.05.2018	3.10	3.4, 4.5	Übertrag in neue Vorlage Kap. 3.4, 4.5 Anpassung Übergang Aufgabe TFM -> TLRZ	G. Weide
01.12.2017	3.0		Freigabe	H. Hartwig
08.12.2016	2.0		Freigabe	H. Hartwig

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
11.09.2015	1.0		Endredaktion und Freigabe	H. Hartwig