



Finanzgruppe Ostdeutscher Sparkassenverband

Programmfreigabe zur Umsetzung der Freigabeverpflichtung nach MaRisk AT7.2

Programmbezeichnung	Maßnahmenbaukasten (GS2025)
Version	1.5
Hersteller/Entwickler	axilaris GmbH Moritzstraße 24 09111 Chemnitz Tel.: 0371-308080 E-mail: support@axilaris.de
Kurzbeschreibung	Der Maßnahmenbaukasten (GS2025) ist die zentrale Anlaufstelle für die operative Umsetzung der Geschäftsstrategie 2025. Er stellt online, übersichtlich und regelmäßig aktualisiert eine Vielzahl praxiserprobter Maßnahmen bereit. Es werden sowohl Good-Practice-Ansätze aus Sparkassen, Konzepte und Unterstützungsleistungen des DSGVO und des OSV, der Verbund- und Netzwerkpartner sowie Schulungsangebote der Nord-Ostdeutschen Sparkassenakademie angeboten.

Hiermit erteilt der OSV (Ostdeutscher Sparkassenverband) als Lieferant die Programmfreigabe für die IT-Anwendung Maßnahmenbaukasten (GS2025).

Details zur Versionierung der IT-Anwendung, deren Herstellungsprozess und Eigenschaften, sowie der Legitimation zu dieser Programmfreigabe ergeben sich aus dem beigefügten Prüfungsbericht der SIZ GmbH als Anlage zur Freigabeerklärung des Herstellers axilaris. Dies ist die Grundlage und der Bestandteil der Freigabeerklärung des OSV.

Die Unterzeichnenden bestätigen die Einhaltung der im Prüfungsbericht benannten Standards und der kaufmännischen Sorgfalt und bestätigen die aus ihrer Sicht korrekte Darstellung der Sachverhalte im Prüfungsbericht.

Alle Maßnahmen, Abstimmungen und Regelungen, die zur Organisation des ordnungsgemäßen Programmeinsatzes erforderlich sind, wurden getroffen und dokumentiert.

Das Programm erfüllt die gestellten Anforderungen hinsichtlich der geplanten Integration in die bestehenden Systemumgebungen der Institute sowie des Datenschutzes.

Das Programm erfüllt aus fachlicher und technischer Sicht die gestellten Anforderungen.

Die Funktionsfähigkeit wurde mit durchgeführten Tests belegt und dokumentiert.

Für die Nutzung des Maßnahmenbaukastens wurden Anwenderhandbücher und Arbeitshilfen bereitgestellt.

Bahly, 5.10.2022

Ort, Datum

Leiter Organisation und IT

Verbandsgeschäftsführer

Anlage: Programmfreigabeerklärung Axilaris incl. SIZ-Bericht

Programmfreigabe zur Umsetzung der Freigabeverpflichtung nach MaRisk AT7.2

Maßnahmenbaukasten (GS2025)

Programmbezeichnung	Maßnahmenbaukasten (GS2025)
Version	1.5
Hersteller/Entwickler	axilaris GmbH Moritzstraße 24 09111 Chemnitz Tel.: 0371-308080 E-mail: support@axilaris.de
Kurzbeschreibung	<p>Der Maßnahmenbaukasten stellt übersichtlich und laufend aktualisiert eine Vielzahl von praxiserprobten Maßnahmen bereit. Außerdem werden ergänzende Unterlagen zu den Einzelmaßnahmen bereitgestellt. Integriert sind ebenso Good-Practice-Ansätze der Sparkassen.</p> <p>Nutzern können dabei nicht nur Maßnahmen, Themen, strategische Ziele, Analysen, Schriften des OSV einsehen und ggf. downloaden, sondern ebenso eigene Dateien hochladen.</p> <p>Der Maßnahmenbaukasten ist eine browserbasierte Anwendung</p>

Hiermit erteilt die axilaris GmbH als Hersteller die Programmfreigabe für die IT-Anwendung Maßnahmenbaukasten (GS2025).

Details zur Versionierung der IT-Anwendung, deren Herstellungsprozess und Eigenschaften, sowie der Legitimation zu dieser Programmfreigabe ergeben sich aus dem beigefügten Prüfungsbericht der SIZ GmbH. Dieser Prüfungsbericht ist Bestandteil der Freigabeerklärung.

Die Unterzeichnenden bestätigen die Einhaltung der im Prüfungsbericht benannten Standards und der kaufmännischen Sorgfalt und bestätigen die aus seiner Sicht korrekte Darstellung der Sachverhalte im Prüfungsbericht.

Das bei uns definierte Verfahren zur qualitätsgesicherten Erstellung von Programmen wurde in allen Punkten eingehalten. Alle Maßnahmen, Abstimmungen und Regelungen, die zur Organisation des ordnungsgemäßen Programmeinsatzes erforderlich sind, wurden getroffen und dokumentiert.

Das Programm erfüllt die gestellten Anforderungen hinsichtlich der geplanten Integration in die bestehenden Systemumgebungen der Institute sowie des Datenschutzes.

Das Programm erfüllt aus fachlicher und technischer Sicht die gestellten Anforderungen. Von der Funktionsfähigkeit haben wir uns überzeugt und die durchgeführten Tests entsprechend unseren Vorgaben dokumentiert.

Zur Anwendung des Programms erforderliche Unterlagen sind bereitgestellt. Anwender-Handbücher bzw. Arbeitshilfen sind vorhanden.

Chemnitz 27.9.2022

Ort, Datum

 Th. Schumann

axilaris GmbH



Inhaltsverzeichnis

1 Prüfungsgegenstand und Verantwortlichkeiten	5
1.1 Identifikation des Prüfungsgegenstandes.....	5
1.2 Fachliche Funktionen des Prüfungsgegenstandes.....	5
1.3 Technische Struktur des Prüfungsgegenstandes	6
1.4 Verantwortung des Auftraggebers der Prüfung.....	8
1.5 Verantwortung des Prüfers.....	9
1.6 Verantwortung des Finanzinstitutes (Auflagen)	12
2 Prüfungsauftrag, sein Inhalt und die Prüfungsdurchführung	14
2.1 Prüfungskriterien	15
2.1.1 Prüfungskriterien aus dem Schutzbedarf	21
3 Ordnungsmäßigkeit und Sicherheit der Programmfunktionen	23
3.1 Ordnungsmäßigkeit nach GoBD/HGB (A+F)	23
3.1.1 Produktbeschreibung und Handbücher	24
3.1.1.1 Technische Struktur	24
3.1.1.2 Rahmenbedingungen.....	24
3.1.1.3 Betriebsaufrechterhaltung	24
3.1.2 GoBD-Verfahrensdokumentation / Dokumentation	24
3.1.3 Verfügbarkeit (Datensicherung, Notfall).....	24
3.1.3.1 K255 Business Continuity und ähnliche Themen der Verfügbarkeit	25
3.1.3.2 K318 Datensicherung.....	26
3.1.4 Integrität (Zugriffskontrollen, Archivierung).....	28
3.1.4.1 K020 Aufbewahrung und Archivierung	28
3.1.4.2 K115 Zugriffsberechtigung	28
3.1.5 Kontrollmaßnahmen / IKS [IDW PS 951, Tz33]	31
3.1.5.1 Technische Kontrollen durch die Software (Plausibilisierung)	31
3.1.5.2 Kontrolle der Berechtigungen	31
3.1.5.3 Eingabe- und Verarbeitungskontrollen für Tätigkeiten	31
3.2 Sicherheit (A+F) in der IT-Anwendung und deren Betrieb.....	31
3.2.1 A020 Sicherheitskonzept / Sollmaßnahmen festlegen.....	31
3.2.1.1 Inhalte des Sicherheitskonzeptes.....	32
3.2.2 K001 IS-Rollen und IS-Gremien (für Provider)	36
3.2.2.1 Der ISB (für Provider)	36
3.2.2.2 Das Team (für Provider)	37
3.2.2.3 Das Reporting (für Provider).....	37
3.2.3 K017 Sichere Administration	37
3.2.4 K018 Trennung der Umgebungen	37
3.2.5 K024, K025 Schulungen, auch IS-Schulung und IS-Sensibilisierung (nur Betreiber)	38
3.2.6 K026 Versicherungen (nur Betreiber)	38
3.2.7 K029 Informationsklassifizierung.....	38
3.2.8 K031 Informationssicherheitsleitlinie (IS-Leitlinie)	39
3.2.9 K033 Personalpolitik.....	39
3.2.10 K034 Audits	40

3.2.11	K050 IT-Strategie.....	40
3.2.12	K106 Datenübertragung.....	40
3.2.12.1	K354 Analoger Datenaustausch	41
3.2.13	K107 Datenablage	41
3.2.13.1	K117 Online-Speicher.....	41
3.2.14	K108 Kryptokonzept	44
3.2.15	K109 E-Mail-Kommunikation.....	44
3.2.16	K110 Protokollierung.....	45
3.2.17	K112 Härtung	46
3.2.18	K113 Schutz vor Schadsoftware	46
3.2.19	K120 Sichere interne Netze (nur Betreiber)	47
3.2.20	K121 Anbindung externer Netze (nur Betreiber)	47
3.2.21	K126 Erkennbarkeit von Angriffen.....	48
3.2.22	K130+131 Virtualisierung (für Provider)	48
3.2.23	K201 Standort, Gebäude, Räume (für Provider)	48
3.2.24	K214 Entsorgung von Datenträgern (nur Betreiber)	51
3.2.25	K215 Transport von digitalen Datenträgern (nur Betreiber).....	51
3.2.26	K309 Dienstleistersteuerung (nur Betreiber bei Auslagerung)	51
3.2.27	K311 Compliance-	52
3.2.28	K329 Changemanagement.....	52
3.2.29	K337 Sicherheitsvorfall-Management (für Provider)	52
3.2.30	K338 Management technischer Schwachstellen	53
3.2.31	K341 Penetrationstest.....	54
3.2.32	K401 Übergreifendes Risikomanagement (nur Betreiber)	54
4	weitere Gesetze, Verordnungen, Standards ... mit IT-Bezug	54
4.1	BDSG/DSGVO	54
4.1.1	BDSG/DSGVO (Ergänzung für Provider und Supportdienstleister)	58
4.1.1.1	Umsetzung der IDW PH 9.860.1.....	59
4.2	BetrVG (zu Kontrollmöglichkeiten über Institutsmitarbeiter)	62
4.3	GeschGehG	62
4.4	LkSG (Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten / Lieferkettensorgfaltspflichtengesetz)	62
4.5	MaRisk (Mindestanforderungen an das Risikomanagement).....	62
4.5.1	AT9 (Auslagerungen).....	62
4.5.2	Anforderungen an einen ordnungsgemäßen Programmeinsatz (bei Modifikationsmöglichkeiten im Institut)	62
4.6	PCI DSS	62
4.7	ProdSichG	62
4.8	StGB 63	
4.9	UrhG 63	
4.10	VSBG (Verbraucherstreitbeilegungsgesetz)	63
5	weitere spezifische Branchen- und Industriestandards.....	64

5.1 AGG	64
5.2 IDW PS 850 (Projektbegleitende Prüfung bei Einsatz von Informationstechnologie)	64
5.2.1 Datenmigration	64
5.3 IDW PS 860 (IT-Prüfung außerhalb der Abschlussprüfung)	64
5.4 IDW PS 951	65
6 organisatorische und technologische Entwicklungsrahmenbedingungen	65
6.1 A001 Organisation festlegen und pflegen	65
6.2 K015 Dokumentations-Anforderungen	66
6.3 K024, K025 Schulungen und Sensibilisierungen	66
6.4 K113 Schutz vor Schadsoftware	67
6.5 K115, K209 Zutritts- und Zugriffsschutz auf der Entwicklungs- und QS-Infrastruktur	67
6.6 K121 Anbindung externer Netze	67
6.7 K346, K341 Anwendungsentwicklung bis Freigabe	67
6.7.1 Anforderungsmanagement im Bereitstellungsprozess (A)	67
6.7.1.1 Berücksichtigung von Fremdkomponenten	68
6.7.2 Design im Bereitstellungsprozess (A)	68
6.7.3 Programmierung im Bereitstellungsprozess (A)	68
6.7.4 Testen im Bereitstellungsprozess (A) [IDW PS 951, Tz9]	69
6.7.4.1 Lasttest	70
6.7.5 Risikomanagement und Projektleitung	70
6.7.6 Versionsverwaltung und Identifikation der IT-Anwendung	71
6.7.6.1 Version der Handbücher	71
6.7.6.2 Version der Testprotokolle und Freigabeerklärungen	71
6.7.7 Wartungs- und Supportmaßnahmen	71
6.7.8 inhaltliche Testabdeckung in Testprotokollen	71
6.7.9 formale Testdokumentation	71
7 Nachweise von Dritten	72
7.1 Allgemeine Nachweise (Nutzer, Rechenzentren, etc.)	72
7.2 Nachweise nach VDG, eIDAS etc.	72
7.2.1 Fallspezifisch empfohlene Fremd-Zertifizierungen	72
7.3 Nachweise zu ISO-, EN- oder DIN-Normen (z.B. 9001, 27001)	72
7.4 Nachweise durch Tätigkeiten des Prüfers der hier dokumentierten Prüfung	72
8 Anlagen	74
8.1 Literaturverzeichnis	74
8.2 Schutzbedarfsanalyse durch den Hersteller respektive Lieferanten	81
8.3 Bestätigung der gesetzlichen Vertreter	81
8.4 Vorschlag einer Freigabeerklärung durch den Lieferanten oder Hersteller	83

8.5 Informationen für den Datenschutzbeauftragten.....	84
8.6 Checkliste zur Unterlageneinreichung	89
8.7 GLOSSAR	103
8.8 INDEX.....	107
9 Unterschrift.....	118

©  GmbH Bonn, 2022

Diese Dokumentation enthält neben Erläuterungen, Bewertungen und eigenen Erhebungen Beschreibungen von Herstellerprodukten, Schnittstellen und Konzepten, die auf entsprechenden Veröffentlichungen der jeweiligen Hersteller beruhen. Sofern in der Dokumentation der SIZ GmbH besondere Geschäfts- oder Betriebsgeheimnisse von Herstellern offengelegt wurden, sind diese in der Dokumentation entsprechend gekennzeichnet und unterliegen damit der besonderen Geheimhaltung.