finma

Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Prüfpunkte Business Continuity Management (BCM)

Versicherungsunternehmen:	
Prüfgesellschaft	
Leitender Prüfer	
Abschluss der Prüfungshandlungen am	
Geschäftsjahr	2023
Version Prüfpunkte Vorlage	27.09.2023

Prüfpunkte Business Continuity Management (BCM)

Version Geschäftsjahr 2023

VU:

Genereller Hinweis für die Prüfer: Der Prüfer ist verpflichtet, die Prüfung mit einer kritischen Grundhaltung vorzubereiten und durchzuführen. Der Prüfer stellt objektive Beurteilungen sicher.

A Prüffeld: Operationalisierung und Führung

		Prüftiefe	Trifft zu	Trifft nicht zu	Erläuterungen	Art	Klassifizierung
A1	Das Versicherungsunternehmen legt in der Geschäftsstrategie und/oder Risikomanagementstrategie die Grundlagen zum Business Continuity Management dar.	Kritische Beurteilung					
A2	Das Versicherungsunternehmen hat die Aufgaben, Kompetenzen und Verantwortlichkeiten der Business Continuity Management Funktion (inklusive der für das BCM notwendigen, weiteren Funktionen und Gremien) klar beschrieben und sorgt mittels geeigneter Massnahmen (z.B. ausreichende Kompetenzen, Ressourcen, Ausbildung) dafür, dass die Funktion wie beschrieben agieren kann. Die Business Continuity Management Funktion und Organisation ist der Grösse, Komplexität und dem Risikoprofil des Unternehmens angepasst.	Kritische Beurteilung					
A3	Das Versicherungsunternehmen hat die internen Bewilligungs- und Berichterstattungspflichten klar geregelt (was wird von wem verabschiedet / was wird wem mit welcher Periodizität in welchem Fall rapportiert).	Kritische Beurteilung					
A4	Die Interne Revision oder eine entsprechende unabhängige Stelle überprüft regelmässig die Einhaltung der Mindeststandards.	Kritische Beurteilung					

B Prüffeld: Business Impact Analyse

			Trifft zu	Trifft nicht zu	Erläuterungen	Art	Klassifizierung
B1	Das Versicherungsunternehmen hat im Rahmen der Erstellung der Business Impact Analyse die wichtigen und zeitkritischen Geschäftsprozesse analysiert. Die für die Durchführung einer Business Impact Analyse notwendigen Inhalte sind definiert. Die für den Betrieb des Versicherungsunternehmens notwendigen Prozesse sind in die Analyse eingeflossen und die relevanten Abhängigkeiten zwischen den Geschäftsprozessen sind berücksichtigt (Prozessabhängigkeiten).	Prüfung					
B2	Für die im Rahmen der Analyse berücksichtigten Prozesse werden die Auswirkungen eines Ausfalls beurteilt. Die Analyse berücksichtigt mindestens die Konsequenzen auf - auf den Betrieb - die Finanzen - die Reputation und - die Einhaltung von Gesetzen und Vorschriften (Compliance).	Prüfung					
B3	Die Business Impact Analyse wurde innerhalb der letzten 3 Jahre mindestens einmal durchgeführt.	Kritische Beurteilung					
B4	Das Versicherungsunternehmen hat Kriterien definiert, aufgrund welcher eine ad-hoc Business Impact Analyse ausserhalb des normalen Aktualisierungszyklus ausgelöst wird (z.B. neue Produkte / Geschäftsfelder / Veränderungen an der IT Infrastruktur, Veränderungen an Prozessen).	Kritische Beurteilung					

C Prüffeld: Business Continuity Strategie

			Trifft zu	Trifft nicht zu	Erläuterungen	Art	Klassifizierung
C1	Das Versicherungsunternehmen hat eine Business Continuity Strategie erstellt, welche sich auf die Erkenntnisse aus der Business Impact Analyse abstützt.	Kritische Beurteilung					

C2	Die aufgrund der Business Impact Analyse als relevant eingestuften Geschäftsbereiche sind in der Business Continuity Strategie bezeichnet.	Prüfung					
C3	Die maximal tolerierbaren Ausfallzeiten pro relevantem Betriebsprozess (gemäss Business Impact Analyse) sind in der Business Continuity Strategie aufgrund ihrer Kritikalität definiert.	Kritische Beurteilung					
C4	Die grundsätzlichen Handlungsoptionen im Ereignisfall sind in der Business Continuity Strategie festgelegt. Der Umfang der Business Continuity Massnahmen für die Bereiche Personal, Infrastruktur, Technik/Telekommunikation und in Bezug auf externe Dienstleister (Outsourcing-Partner) ist festgelegt.	Kritische Beurteilung					
C5	In der Business Continuity Strategie sind konkrete Vorgaben/Kriterien definiert, in welchen Fällen die Auswirkungen ohne vorbereitete Überbrückungs- und Wiederherstellungsmassnahmen akzeptiert werden.	Kritische Beurteilung					

D Prüffeld: Business Continuity Massnahmen

			Trifft zu	Trifft nicht zu	Erläuterungen	Art	Klassifizierung
D1	Business Continuity Massnahmen sind für die gemäss Business Continuity Strategie wichtigen und zeitkritischen Geschäftsprozesse definiert.	Prüfung					
D2	Die Business Continuity Massnahmen berücksichtigen das Vorgehen, die Mittel und notwendigen Ressourcen zur Überbrückung und Wiederherstellung der wichtigen und zeitkritischen Geschäftsprozesse.	Prüfung					
D3	Das Versicherungsunternehmen hat nachvollziehbar festgelegt, wie alle betroffenen Geschäftsbereiche/Mitarbeitenden über die Business Continuity Massnahmen informiert und geschult werden.	Kritische Beurteilung					

E Prüffeld: Übungen und Tests

			Trifft zu	Trifft nicht zu	Erläuterungen	Art	Klassifizierung
E1	Das Versicherungsunternehmen hat Übungs- und Testverfahren definiert. Die Verfahren berücksichtigen die im Rahmen der Business Impact Analyse und Business Continuity Strategie identifizierten wichtigen und zeitkritischen Geschäftsprozesse und definiert welche Massnahmen wann, wie und wie oft getestet werden.	Kritische Beurteilung					
E2	Die Periodizität für die Durchführung von Übungen und Tests ist definiert und im Kontext zum Risikoprofil, der Grösse und Komplexität des Versicherungsunternehmens angemessen.	Kritische Beurteilung					
E3	Die Übungs- und Testergebnisse sind nachvollziehbar dokumentiert.	Prüfung					
E4	Das Versicherungsunternehmen stellt mittels geeigneter Massnahmen sicher, dass die aus den Übungen und Tests erkannten Schwachstellen beurteilt und mittels Verbesserungsmassnahmen adressiert werden. Der Business Continuity Management Organisation wird darüber Bericht erstattet.	Kritische Beurteilung					

F Ergänzende Angaben zum Prüfgebiet

					Erläuterungen		
F1	Der Prüfer wird gebeten, kurz zu umschreiben, wo die Verantwortung für das BCM organisatorisch eingegliedert ist und die verantwortliche(n) Person(en) zu benennen						
F2	Der Prüfer wird gebeten, in den Erläuterungen anzugeben, per wann die letzte Überprüfung durch die Interne Revision stattgefunden hat, was das Resultat dieser Überprüfung war und wie hoch die Prüffrequenz gemäss Mehrjahresprüfplan ist.						
F3	Der Prüfer wird gebeten, die in der Business Impact Analyse als zeitkritisch eingestuften Geschäftsprozesse in den Erläuterungen aufzulisten.						
F4	Haben vergangenen Betriebseinschränkungen/-unterbrüche (bspw. Stromausfall, Cyber Angriff, Pandemie etc.) zu Business Continuity Massnahmen und einer Anpassung am BIA geführt? Beschreiben sie kurz, ob und welche Anpassungen dadurch am BCM vorgenommen wurden.						