

Inhaltsverzeichnis

1 Einleitung	1
1.1 Ausgangssituation und Problemstellung	1
1.1.1 Grundlegende Begrifflichkeiten	3
1.1.2 BCBS 239	5
1.1.2.1 Risikodatenaggregation	5
1.1.2.2 Auswirkungen auf andere Aufsichtsmandate und Behörden	7
1.1.2.3 Laufende Überprüfung der Umsetzung durch den BCBS	9
1.1.2.4 Analyse der Erfüllungsgrade seit 2013	10
1.1.3 IT-Bedrohungslage	13
1.2 Schwerpunkte der Arbeit	15
1.2.1 Governance	16
1.2.2 Fachwissen	19
1.2.3 Aktuelle IT-Sicherheitstechnik	20
1.3 Leitende Forschungsfragestellung	22
1.4 Aufbau und Struktur der Arbeit	23
1.5 Zusammenfassung Kapitel 1	26
2 Literaturüberblick	27
2.1 Theoretischer Bezugsrahmen	28
2.2 Durchführung Literaturüberblick	29
2.2.1 Methodische Vorgehensweise	29
2.2.1.1 Überprüfung der Charakterisierungskategorien	29
2.2.1.2 Phasen der Reviewforschung	31

2.2.2	Strategie der Literatursuche	31
2.2.2.1	Suchbegriffe	31
2.2.2.2	Ein- und Ausschlusskriterien	32
2.2.2.3	Datenextraktion	33
2.2.3	Auswertung der Literatur	33
2.2.4	Analyse und Interpretation der Literatur	34
2.2.4.1	Literaturüberblick über künstliche Intelligenz und Machine-Learning	34
2.2.4.2	Literaturüberblick zu Governance und IT-Fachwissen	52
2.2.4.3	Schlussfolgerung zur Analyse und Interpretation der Literatur	55
2.3	Ergebnisse und Erkenntnis	56
2.3.1	Künstliche Intelligenz und Machine-Learning	56
2.3.2	Governance und IT-Fachwissen	57
2.3.3	Ergebnisse in Relation zu den Grundsätzen des BCBS 239	58
2.3.4	Zusammenfassung Ergebnisse und Erkenntnis	60
2.4	Forschungslücke	61
2.4.1	Motivation	61
2.4.1.1	Digitalisierung	61
2.4.1.2	IT-Sicherheitslage	63
2.4.1.3	Konsequenzen aus IT-Sicherheitsvorfällen	64
2.4.2	Existierende Ansätze in der Literatur	65
2.4.2.1	Ansätze zum Schwerpunkt ‚Governance‘	65
2.4.2.2	Ansätze zum Schwerpunkt ‚Fachwissen‘	66
2.4.2.3	Ansätze zum Schwerpunkt ‚aktuelle Sicherheitstechnik‘ (KI/ML)	66
2.4.3	Noch nicht erforschte Zusammenhänge	67
2.4.4	Eingrenzungen der Forschungsarbeit	67
2.5	Forschungsfragen	68
3	Methodik	71
3.1	Forschungsziele	73
3.2	Forschungsdesign	75
3.2.1	Design Science Research	76
3.2.1.1	Grundsätze von Design Science Research für die Forschungsarbeit	77
3.2.1.2	Artefaktentwicklung	78

3.2.1.3	Theoretische Grundlagen der Arbeit	79
3.2.1.4	Zuverlässigkeit und Validität	83
3.2.1.5	Einordnung des Forschungsdesigns der Arbeit	89
3.2.2	Datenerhebung und -auswertung	90
3.2.2.1	Literaturüberblick	91
3.2.2.2	Qualitative Untersuchung	91
3.2.2.3	Quantitative Untersuchung	91
3.2.2.4	Ethische Vorgehensweisen	92
3.2.2.5	Teilnehmerauswahl	92
3.2.2.6	Technische Ausstattung	93
3.2.2.7	Analyseverfahren	94
3.2.3	Rolle des Forschers	95
4	Empirische Erhebungen	97
4.1	Qualitative Erhebung	97
4.1.1	Theorie zur Art der qualitativen Erhebung	98
4.1.2	Durchführung und Rahmenbedingungen	99
4.1.2.1	Demografische Daten der befragten Personen	100
4.1.2.2	Vorgehen bei der Auswertung	102
4.1.2.3	Schlagwortwolke	102
4.1.2.4	Erstellung Codierungsagenda nach Mayring	103
4.1.3	Ergebnisse und Implikationen für das weitere Vorgehen	105
4.1.3.1	Kategorie 1: Stellenwert der IT-Sicherheitstechnik	105
4.1.3.2	Kategorie 2: Einfluss technisch-organisatorischer Strukturen	106
4.1.3.3	Kategorie 3: IT-Sicherheitsniveau bei internen und externen UZV	108
4.1.3.4	Kategorie 4: Einfluss des IT-Fachwissens	110
4.1.3.5	Kategorie 5: Einfluss aktueller IT-Sicherheitstechnik	112
4.1.4	Ableitung der Hypothesen	115
4.1.5	Fazit der qualitativen Erhebung	120
4.1.6	Vorläufige Darstellung der Solution Architecture	121

4.2	Quantitative Erhebung	124
4.2.1	Theoretische Grundlage der quantitativen Erhebung	125
4.2.1.1	Erstellung der Umfrage	125
4.2.1.2	Analyseverfahren	125
4.2.1.3	Vorteile der gewählten Verfahren	129
4.2.1.4	Einschränkungen des gewählten Verfahrens	129
4.2.2	Durchführung und Rahmenbedingungen	130
4.2.3	Ergebnisse	136
4.2.3.1	Repräsentativität und Aussagekraft der Ergebnisse	136
4.2.3.2	Gruppierung der Fragen	139
4.2.3.3	Auswertung der Fragen	140
4.2.3.4	Prüfung auf Konstruktreliabilität	172
4.2.4	Hypothesenüberprüfung	175
5	Ergebnisse	179
5.1	Lösungsansätze	179
5.1.1	Lösungsansätze aus der qualitativen Erhebung	180
5.1.2	Lösungsansätze aus der quantitativen Erhebung	181
5.2	Artefaktentwicklung	181
5.2.1	Beschreibung DSR-Artefaktentwicklung	181
5.2.2	Build-Prozess der Artefaktentwicklung	182
5.3	Architekturentwicklung	182
5.3.1	Entwicklungsumfeld der Solution Architecture	183
5.3.2	Governance	185
5.3.3	Risikodatenarchitektur	186
5.3.4	IT-Infrastruktur	188
5.3.5	Interaktion zwischen den Elementen der Solution Architecture	191
5.3.6	Erwartete Herausforderungen	194
5.3.7	Schlussfolgerung	195
5.3.8	Darstellung Solution Architecture	196
5.4	Zusammenfassung der Ergebnisse	196
6	Überprüfung der Lösungsansätze	199
6.1	Evaluate-Prozess der Artefaktentwicklung	199
6.2	Iterationen der Solution Architecture	201
6.3	Praxisbasierte Überprüfung der Solution Architecture	203

7 Diskussion	211
7.1 Interpretation der Ergebnisse	211
7.2 Einschränkungen der Forschungsarbeit	217
7.3 Empfehlungen	219
7.4 Weiterer Forschungsbedarf	221
7.5 Schlussfolgerungen	222
Literaturverzeichnis	227