

Riediger (Hrsg.)

Auslagerungen und Dienstleister- Steuerung

Aktuelle Anforderungen aus DORA, KWG, EBA-Guidelines
und MaRisk/BAIT im Umgang mit Auslagerungen für
signifikante und weniger signifikante Institute

3. Auflage

Riediger (Hrsg.)

Auslagerungen und Dienstleister- Steuerung

**Aktuelle Anforderungen aus DORA, KWG, EBA-Guidelines
und MaRisk/BAIT im Umgang mit Auslagerungen für
signifikante und weniger signifikante Institute**

3. Auflage

Khalid Ahmad

DOR-Beauftragter
Abteilungsleiter Business Resilience
Deutsche WertpapierService Bank AG

Sven Chudzinski

Bereichsleiter Controlling, Meldewesen und
Zentrales Auslagerungsmanagement
Volksbank im Bergischen Land eG

Larissa Eigenwillig

Consultant Kompetenzteam Compliance
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Michael Gastmann

Auslagerungsbeauftragter/Datenschutzbeauftragter
Stabsstelle Überwachungsmanagement
Volksbank im Münsterland eG

Roland Hein

Geschäftsführer
bit Informatik GmbH

Maximilian Herting

Wissenschaftlicher Mitarbeiter
AWADO Rechtsanwaltsgesellschaft mbH &
Universität Osnabrück

Johannes Hugo

Leiter Competence Center Information Security
x1F GmbH

Barbara Hugo-Dilworth

Head of Outsourcing Management
IKB Deutsche Industriebank AG

Michael Kirschbaum

Referent Zentrales Auslagerungsmanagement
LBBW

Daniel Krüger

Rechtsanwalt
AWADO Rechtsanwaltsgesellschaft mbH

Christoph Leibnitz

Zentraler Auslagerungsbeauftragter
Sparkasse Mülheim an der Ruhr

Oliver Michelmann

Fachprüfer im Referat Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Hannover

Markus Müller

Independent Compliance Risk Management
Germany MaRisk-Compliance Monitoring/
Deputy Head MaRisk-Compliance
Citigroup Global Markets Deutschland AG

Stefan Nikula

Abteilungsleiter Gesamtbanksteuerung
Salzlandsparkasse

Henning Riediger (Hrsg.)

Prüfungsleiter, Referat Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Hannover

Pascal Ritz LL.M.

Geschäftsführer
Justo Unternehmensberatung GmbH
Compliance-Spezialist

Ingvar Rosenhagen

Bereichsleiter IT-Governance
ALTE LEIPZIGER Lebensversicherung auf Gegenseitigkeit

Selina Schubert, LL.M.

Consultant Kompetenzteam Compliance
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Kathrin Stein

Leiterin Interne Revision
Sparda-Bank München eG

Peter Uherr

Director, Leiter Compliance
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Kay Wachelau

Auslagerungsbeauftragter | Beauftragter für IKT-Drittparteien
DONNER & REUSCHEL Aktiengesellschaft

FCH AG, 2025

Inhaltsübersicht

| | |
|--|-----|
| A. Einleitung | 1 |
| B. Begriffsbestimmung und Abgrenzungstatbestand | 9 |
| C. Risikoanalysen zur Wesentlichkeitseinstufung von Auslagerungen | 83 |
| D. Integration von DORA in den Auslagerungsprozess | 177 |
| E. Aufbau einer Dienstleistersteuerung | 241 |
| F. Auslagerbarkeit von Kontroll- und Kernbereichen | 317 |
| G. Auslagerung der IT-Sicherheitsfunktionen bzw. deren Überwachung | 339 |
| H. Integration von Auslagerungen in das Interne Kontrollsystem und das Zusammenwirken von Beauftragten | 369 |
| I. Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen an Auslagerungen | 399 |
| J. Handlungsoptionen und Notfallpläne bei Beendigung einer Auslagerung | 427 |
| K. Berücksichtigung von Weiterverlagerungen | 451 |
| L. Überwachung von Dienstleistern unter Berücksichtigung der Proportionalität bei SI und LSI | 469 |

| | |
|---|------------|
| M. Plausibilitäts- und Prüfungspflichten der Internen Revision vor, während und nach der Auslagerung | 537 |
| N. Bankaufsichtliche Überwachung von Auslagerungsprozessen | 579 |
| Literaturverzeichnis | 589 |
| Stichwortverzeichnis | 601 |

Inhaltsverzeichnis

| | |
|---|----------|
| A. Einleitung <i>(Riediger)</i> | 1 |
| I. Vorüberlegungen | 3 |
| II. Aufbau des Werkes | 4 |
| B. Begriffsbestimmung und Abgrenzungstatbestand | 9 |
| I. Bedeutung der Auslagerung im Internen Kontrollsystem <i>(Riediger)</i> | 11 |
| 1. Vorbemerkungen | 11 |
| 2. Abgrenzung Auslagerung und Fremdbezug | 15 |
| 3. Strategische Vorgaben zum Umgang mit Risiken aus Auslagerungen und Standards | 18 |
| 4. Risikoinventur und Risikoanalysen | 20 |
| II. Schwerpunkt bei Auslagerungsthemen sind die Informationstechnologie und deren Schnittstellen <i>(Riediger)</i> | 24 |
| 1. Allgemeine Aspekte | 24 |
| 2. Einbindung von IT-Auslagerungen in das Informationsrisikomanagement | 28 |
| 3. Schnittstelle zum Benutzerberechtigungsmanagement | 36 |
| 4. Schnittstellen zum Notfallmanagement | 39 |
| III. Überwachung des Dienstleisters <i>(Riediger)</i> | 42 |
| 1. Auslagerungsüberwachung im Internen Kontrollsystem | 45 |
| 2. Überprüfung der Auslagerung durch die Interne Revision | 51 |
| IV. EBA-Guideline 2019/02 <i>(Riediger)</i> | 56 |
| 1. Auslagerungsbegriff | 56 |
| 2. Auslagerungsregister | 57 |
| 3. Auslagerungsbegriff Zugangs-, Informations- und Prüfungsrechte | 59 |
| 4. Interessenskonflikte | 59 |

| | | |
|-----------|---|-----------|
| V. | Herausforderungen für das Auslagerungsmanagement und die digitale Transformation durch DORA (<i>Michelmann</i>) | 62 |
| 1. | Einleitung | 62 |
| 2. | Herausforderungen von DORA für Auslagerungen | 63 |
| 3. | Potenzielle Auswirkungen von DORA auf die digitale Transformation | 65 |
| 4. | Fazit | 78 |
| C. | Risikoanalysen zur Wesentlichkeitseinstufung von Auslagerungen | 83 |
| I. | Risikoanalysen am Beispiel eines LSI (<i>Nikula</i>) | 85 |
| 1. | Ziele Einstufung in wesentliche und nicht wesentliche Auslagerungen | 85 |
| 2. | Auslagerungs-, Weiterverlagerungs- und Konzentrationsrisiken | 101 |
| 3. | Durchführung regelmäßiger und anlassbezogener Risikoanalysen | 103 |
| 4. | Ablauf einer Risikoanalyse in Anlehnung an den Risikoinventur-Prozess | 109 |
| 5. | Einbindung maßgeblicher Organisationseinheiten | 113 |
| 6. | Überführung der Analyse-Ergebnisse in das Risikotragfähigkeitskonzept | 115 |
| II. | Risikoanalysen am Beispiel eines SI (<i>Abmad/Kirschbaum</i>) | 120 |
| 1. | Überblick relevante rechtliche und regulatorische Grundlagen zur Risikobewertung und deren Geltungsbereich | 120 |
| 2. | Aufbauorganisation und Three-Lines-of-Defense-Modell im Auslagerungsmanagement | 138 |
| 3. | Zielsetzung der Auslagerungsrisikobewertung | 142 |
| 4. | Intern orientierte Risikobewertung | 149 |
| 5. | Extern orientierte Risikobewertung (Auslagerungsrisikobewertung gem. Tz. 12.2/12.3 der EBA GL 2019/02) | 156 |

| | | |
|---|--|------------|
| 6. | Einbindung von Querschnittsthemen | 159 |
| 7. | Bewertung der Risiken im Rahmen der Auslagerungsrisikobewertung | 161 |
| 8. | Wirkung der Weiterverlagerung auf die originäre Risikobewertung | 167 |
| 9. | Auswirkung der Risikobewertung auf die Steuerung der Auslagerung | 168 |
| 10. | Auswirkung der Wesentlichkeit auf die Exit-Strategie | 169 |
| 11. | Aktualisierung der Auslagerungsrisikobewertung | 170 |
| 12. | Wichtige Anzeigepflichten, Dokumentationsanforderungen und Berichtspflichten im Zusammenhang mit der Risikobewertung | 174 |
| 13. | Wichtige Anzeigepflichten, Dokumentationsanforderungen und Berichtspflichten im Zusammenhang mit der Risikobewertung | 175 |
| D. Integration von DORA in den Auslagerungsprozess (<i>Hein</i>) | | 177 |
| I. | Einführung | 179 |
| 1. | Ziele von DORA | 180 |
| 2. | Erläuterung von DORA an einem konkreten Dienstleister | 180 |
| 3. | Vergleich von DORA zu nationalen aufsichtsrechtlichen Anforderungen – Gegenüberstellung DORA und MaRisk/BAIT | 181 |
| 4. | Auslagerung ist grundsätzlich sinnvoll | 190 |
| 5. | Erläuterung der wesentlichen Anforderung von DORA | 191 |
| II. | IST-Analyse – Zusammentragen und Sichtung aller heutigen Dienstleisterverträge | 197 |
| 1. | Anforderungen an Auslagerungsverträge | 199 |
| 2. | Aktualität der Verträge – Schwerpunkt allgemeine Informationen | 200 |
| 3. | Festlegungen von zukünftig zu überwachenden Verträgen | 202 |

| | |
|--|-----|
| III. Zuständigkeiten und Verantwortliche | 203 |
| IV. Festlegung der Prozesse | 205 |
| V. Aufbau einer Risikoanalyse | 208 |
| VI. Allgemeine Anforderungen an einen IKT-Dienstleister | 212 |
| 1. Vertrag zur Auftragsdatenverarbeitung | 212 |
| 2. Fernwartungsvertrag | 212 |
| 3. Technische und organisatorische Maßnahmen (TOM) | 212 |
| 4. Escrow (Treuhand) Vertrag | 213 |
| 5. Dokument »Data protection by design« | 213 |
| 6. Verschwiegenheitsvereinbarung | 214 |
| 7. Nachhaltigkeitsbericht | 214 |
| 8. Lieferkettensorgfaltspflichtengesetz | 214 |
| 9. Beispiel für die Bewertung eines Dienstleisters (Kurzbewertung) | 215 |
| VII. Berichtsauswertung – Bearbeitung der Informationspflichten des Dienstleisters | 216 |
| VIII. Weiterverlagerung | 220 |
| IX. Leistungsüberwachung – Anwendung von Service Level Agreements (SLA) | 224 |
| X. Servicegespräche | 229 |
| XI. Bericht an die Geschäftsführung | 230 |
| XII. Aufbau eines Informationsregisters | 232 |
| XIII. Auswertung | 234 |
| XIV. Zugriffsberechtigungen | 235 |
| XV. Fazit | 236 |
| 1. Dienstleister-Steuerung als Chance | 236 |
| 2. Angemessene Personalbesetzung und Ausbildung | 237 |
| 3. Vorstand als Sponsor | 237 |
| 4. Ganzheitlicher Ansatz der Umsetzung aufsichts- rechtlicher Anforderungen aus DORA und MaRisk | 238 |

| | |
|--|------------|
| 5. Ausblick – Entwicklungen in diversen Verbundgruppen | 239 |
| E. Aufbau einer Dienstleistersteuerung | 241 |
| I. Rechtlicher Rahmen – Zusammenspiel der Funktionen <i>(Müller/Rosenbagen)</i> | 243 |
| 1. Einleitung zum Aufbau einer Dienstleistersteuerung | 243 |
| 2. Strategische Überlegungen vor einer Auslagerung | 245 |
| 3. Rahmenbedingungen in modernen Finanz- und Versicherungsinstituten | 250 |
| 4. Anforderungen an den Aufbau einer Dienstleistersteuerung | 254 |
| 5. Rechtliche und Regulatorische Vorgaben | 259 |
| 6. Aufbau einer Dienstleistersteuerung | 267 |
| II. Aus Sicht einer Bank <i>(Wachelaun)</i> | 276 |
| 1. Einführung | 276 |
| 2. (Strategische) Parameter für den Aufbau | 278 |
| 3. Ausgestaltung der Dienstleister-Steuerung | 284 |
| 4. Schnittstellen und Prozesse | 286 |
| 5. Gestaltung des Außenverhältnisses zum Dienstleister | 292 |
| 6. Erfolgsfaktoren | 300 |
| 7. Fazit | 304 |
| III. Aus Sicht einer Versicherung <i>(Müller/Rosenbagen)</i> | 305 |
| 1. Aufbau einer Dienstleistersteuerung aus Sicht einer Versicherung | 305 |
| 2. Anforderungen an die Dienstleistersteuerung im Versicherungskontext | 305 |
| 3. Maßnahmen und Sanktionen der Aufsicht | 313 |
| 4. Auswirkungen auf die Prüfungspraxis – Maßnahmen und Sanktionen | 314 |
| F. Auslagerbarkeit von Kontroll- und Kernbereichen <i>(Uherr/Eigenwillig/Schubert)</i> | 317 |

| | | |
|-----------|--|------------|
| I. | Zulässigkeit von Auslagerungen in Bezug auf Kontroll- und Kernbankbereiche und dessen Voraussetzungen | 319 |
| 1. | Compliance-Funktion | 320 |
| 2. | Interne Revision | 321 |
| 3. | Vertragsgestaltung und SLA | 321 |
| 4. | Risikomanagement und Überwachung | 321 |
| 5. | Krisen- und Notfallmanagement | 321 |
| 6. | Meldepflichten gegenüber der BaFin | 322 |
| II. | Besondere Maßstäbe für Voll-/Teil-Auslagerungen der Kontrollbankbereiche und Erleichterungen für kleinere Institute bei Vollauslagerung insbesondere der Compliance-Funktion | 322 |
| 1. | MaRisk-Compliance-Funktion | 325 |
| 2. | WpHG-Compliance-Funktion | 326 |
| 3. | Geldwäschebeauftragter | 329 |
| III. | Qualität der Verbindungsperson im Haus | 331 |
| IV. | Leistungsüberwachungskriterien von Vertragsvereinbarungen (SLAs) und Überwachung des Reportings | 334 |
| V. | Kritik und Herausforderungen | 337 |
| G. | Auslagerung der IT-Sicherheitsfunktionen bzw. deren Überwachung (<i>Hugo</i>) | 339 |
| I. | Einführung in die Auslagerung sicherheitskritischer IT-Funktionen | 341 |
| 1. | Einleitung | 341 |
| 2. | Gründe für die Auslagerung | 341 |
| 3. | Relevanz der Überwachung bei der Auslagerung | 342 |
| 4. | Erweiterung der regulatorischen Vorgaben und Prüfmechanismen | 342 |
| 5. | Risiken und Statistiken zur Auslagerung | 343 |
| 6. | Zusammenfassung der Einführung | 343 |

| | | |
|------|---|-----|
| II. | Regulatorischer Rahmen: DORA, MaRisk, EBA-Guidelines und BAIT | 343 |
| 1. | Digital Operational Resilience Act (DORA) | 343 |
| 2. | MaRisk – Mindestanforderungen an das Risikomanagement | 344 |
| 3. | EBA-Guidelines on Outsourcing Arrangements | 345 |
| 4. | BAIT – Bankaufsichtliche Anforderungen an die IT | 345 |
| 5. | Zusammenfassung des regulatorischen Rahmens | 345 |
| III. | Überwachung von ausgelagerten Sicherheitsfunktionen | 346 |
| 1. | Identity and Access Management (IAM) | 346 |
| 2. | Privileged Access Management (PAM) | 347 |
| 3. | Security Information and Event Management (SIEM) | 348 |
| 4. | Data Loss Prevention (DLP) | 348 |
| 5. | Vulnerability Management | 349 |
| 6. | Incident Management | 350 |
| IV. | Metriken zur Risikobewertung und Konzentrationsrisiken | 351 |
| 1. | Quantitative Risikobewertung | 351 |
| 2. | Wichtige Metriken zur Risikobewertung je Sicherheitsfunktion | 351 |
| 3. | Konzentrationsrisiken bei Providern | 354 |
| 4. | Szenarien zur Überschreitung des operationellen Risikos (erweitert) | 357 |
| 5. | Einfluss auf die Eigenkapitalhinterlegung – AMA, BIA, SMA (Exkurs) | 358 |
| 6. | Vernetzung von Auslagerungsmanagement, IT-Sicherheit, Compliance und Risikomanagement | 359 |
| 7. | Nutzung eines zentralen Tools zur Überwachung der Sicherheitsfunktionen (erweitert) | 360 |
| 8. | Zusammenfassende Nutzwerttabelle eines Providers mit KPIs und Gewichtung | 362 |
| V. | Zusammenfassung und Ausblick | 365 |
| 1. | Zusammenfassung | 365 |

| | | |
|-----------|--|------------|
| 2. | Ausblick | 365 |
| 3. | Schlussbemerkung | 367 |
| H. | Integration von Auslagerungen in das Interne Kontrollsystem und das Zusammenwirken von Beauftragten <i>(Ritz)</i> | 369 |
| I. | Vorbemerkungen | 371 |
| II. | Beurteilung der Einstufung der Wesentlichkeit von Auslagerungssachverhalten | 373 |
| 1. | Ausfallrisiken | 377 |
| 2. | Rechtsrisiken | 378 |
| 3. | Reputationsrisiken | 379 |
| 4. | Prozessrisiken | 380 |
| 5. | Sicherheitsrisiken | 383 |
| III. | Zulässigkeit von Auslagerungen in Bezug auf Kontroll- und Kernbankbereiche | 384 |
| IV. | Kontrolle der lfd. Leistungsüberwachung von Vertragsvereinbarungen (SLAs) | 385 |
| V. | Überwachung des Reportings der Dienstleister-Steuerung und Auslagerungspartner | 388 |
| VI. | Überwachung Exit Management: Kündigungsrechte, Ausstiegsstrategien, Notfallkonzepte | 392 |
| VII. | Aufbau und Implementierung eines Dienstleister-Internen Kontrollsystems | 394 |
| VIII. | Zusammenfassung und Ausblick | 397 |
| I. | Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen an Auslagerungen <i>(Krüger/ Herting)</i> | 399 |
| I. | Vorbemerkungen | 401 |
| II. | Vorkehrungen für beabsichtigte und erwartete Beendigung der Auslagerungsvereinbarung | 404 |

| | | |
|-----------|---|------------|
| 1. | Ursachen für beabsichtigte und erwartete Beendigungen von Auslagerungen | 404 |
| 2. | Vorkehrungen und Handlungsoptionen im Falle des Eintritts beabsichtigter oder erwarteter Beendigungen von Auslagerungen | 407 |
| III. | Festlegung von Ausstiegsstrategien für die unbeabsichtigte oder unerwartete Beendigung von Auslagerungen | 410 |
| 1. | Ursachen für unbeabsichtigte oder unerwartete Beendigungen von Auslagerungen | 410 |
| 2. | Ausstiegsstrategien | 411 |
| IV. | Handlungsoptionen im Notfallmanagement bei nicht festgelegten Ausstiegsstrategien | 413 |
| 1. | Zeitkritische Aktivitäten und Prozesse | 414 |
| 2. | Inhalt des Notfallkonzepts | 415 |
| 3. | Überprüfungen des Notfallkonzepts | 416 |
| V. | Vereinbarung und Ausgestaltung von Kündigungsrechten für dauerhafte Schlechtleistung | 418 |
| 1. | Überlegungen zur Vermeidung dauerhafter Schlechtleistungen | 418 |
| 2. | Optionen zur Gewährleistung von Handlungsfähigkeiten im Falle dauerhafter Schlechtleistungen | 419 |
| 3. | Anforderungen an ein effektives Vertragsmanagement | 422 |
| J. | Handlungsoptionen und Notfallpläne bei Beendigung einer Auslagerung (<i>Chudziński</i>) | 427 |
| I. | Vorbemerkungen | 429 |
| II. | Anforderungen der MaRisk an Verträge und Prozesse für die Beendigung von Auslagerungen | 429 |
| 1. | Rechtliche Vorgaben aus den MaRisk | 429 |
| 2. | Die Vertragsdatenbank als Medium zur schnellen Informationsbevorratung | 430 |

| | | |
|-----------|--|------------|
| 3. | Die Rolle des zentralen Auslagerungsmanagements und des dezentralen Auslagerungsmanagements im Rahmen des Ausstiegsprozesses | 432 |
| III. | Die geplante Beendigung von Auslagerungen | 432 |
| 1. | Mögliche Gründe für die Kündigung von Auslagerungsvereinbarungen | 432 |
| 2. | Notwendige Anzeigen an die BaFin | 434 |
| 3. | Die beispielhafte Einlagerung eines ausgelagerten Sachverhaltes am Beispiel der Nachlassbearbeitung | 436 |
| IV. | Die ungeplante Beendigung von Auslagerungen | 437 |
| 1. | Mögliche Gründe für die außerordentliche Beendigung von Auslagerungsvereinbarungen | 437 |
| 2. | Notwendige Anzeigen an die BaFin | 439 |
| 3. | Der beispielhafte Umgang mit einer außerordentlichen Auslagerungsbeendigung am Beispiel der Kreditweiterbearbeitung | 443 |
| V. | Berücksichtigung der Auslagerungen im Rahmen der Notfallplanung | 446 |
| 1. | Definition von Notfallplänen und deren aufsichtliche Anforderungen | 446 |
| 2. | Durchführung von Notfalltests | 447 |
| VI. | Fazit | 450 |
| K. | Berücksichtigung von Weiterverlagerungen (<i>Leibnitz</i>) | 451 |
| I. | Vorüberlegungen zu Weiterverlagerungen | 453 |
| II. | Vereinbarung von Zustimmungsvorbehalten zugunsten des auslagernden Instituts | 458 |
| III. | Voraussetzungen für Weiterverlagerungen einzelner Arbeits- und Prozessschritte | 461 |
| IV. | Sicherstellung und Anpassung der Berichtspflichten gegenüber auslagernden Instituten | 463 |
| V. | Fazit | 467 |

| | |
|--|------------|
| L. Überwachung von Dienstleistern unter Berücksichtigung der Proportionalität bei SI und LSI | 469 |
| I. Überwachung der Dienstleister bei LSIs (<i>Gastmann</i>) | 471 |
| 1. Auslagerungssteuerung und -überwachung | 471 |
| 2. Berichtswesen zur Auslagerungssteuerung und -überwachung | 476 |
| 3. Ausblick | 505 |
| II. Drittparteienrisiken in der Gesamtbanksteuerung (<i>Hugo-Dihvorth</i>) | 507 |
| 1. Vorbemerkung | 507 |
| 2. Drittparteienrisiken im Fokus der Aufsicht | 507 |
| 3. Das Drittparteienrisiken im Gesamtrisikoprofil des Instituts | 508 |
| 4. Ableitung des Risikoappetits aus der Risikostrategie | 511 |
| 5. Steuerungs- und -überwachungskreislauf | 513 |
| 6. Gesamtbankberichterstattung über Drittparteienrisiken | 527 |
| 7. Zusammenfassung | 535 |
| M. Plausibilitäts- und Prüfungspflichten der Internen Revision vor, während und nach der Auslagerung (<i>Stein</i>) | 537 |
| I. Vorbemerkung | 539 |
| II. Aktualität der Prüflandkarte – Berücksichtigung von Auslagerungen und IKT-Dienstleisterbeziehungen | 540 |
| 1. Grundlegende Rahmenbedingungen zur Einbindung der Internen Revision | 541 |
| 2. Festlegung von Prüfungsumfang und -turnus | 546 |
| III. Aufbau- und ablauforganisatorischen Grundlagen im Auslagerungs- und Drittparteirisikomanagement | 548 |
| 1. Strategie, Organisationsrichtlinien und Interne Governance | 548 |

| | | |
|------|---|-----|
| 2. | Implementierung und Weiterentwicklung des zentralen Auslagerungsmanagements inklusive Kontroll- und Überwachungsprozesse | 550 |
| IV. | Beurteilung von Risikoanalysen und Risikobewertung | 554 |
| 1. | Koordination durch zentrales Auslagerungsmanagement bzw. Überwachungsfunktion für IKT-Dienstleistungen | 555 |
| 2. | Beurteilungskriterien für Risikoanalyse und Due-Diligence | 555 |
| 3. | Berücksichtigung der Risiken aus Auslagerungen und IKT-Drittparteirischen im Rahmen der operationellen Risiken | 559 |
| 4. | Wirtschaftlichkeitsbetrachtung | 563 |
| V. | Auslagerungs- und Informationsregister – Erstellung und Pflege einer vollständigen Dokumentation der Auslagerungen und IKT-Dienstleistungen | 563 |
| 1. | Auslagerungsregister | 563 |
| 2. | Informationsregister | 565 |
| VI. | Vertragliche Anforderungen für Auslagerungen und IKT-Dienstleister | 567 |
| 1. | Vertragliche Anforderungen nach MaRisk | 567 |
| 2. | Vertragliche Anforderungen unter DORA | 570 |
| VII. | Laufende Auslagerungsüberwachung und Dienstleistersteuerung | 573 |
| 1. | Funktionsfähigkeit der Dienstleister-Revision und Berichtsauswertung in der Internen Revision | 574 |
| 2. | Eigene Prüfung des Dienstleisters | 576 |

| | |
|--|------------|
| N. Bankaufsichtliche Überwachung von Auslagerungsprozessen | 579 |
| <i>(Riediger)</i> | |
| I. Internes Kontrollsystem als maßgebliches Instrument | 581 |
| II. Kapitalzuschläge wegen Mängeln bei Auslagerungen | 583 |
| III. Auslagerungen als Schwerpunkt in Bankgeschäftlichen Prüfungen der Aufsicht | 586 |
| Literaturverzeichnis | 589 |
| Stichwortverzeichnis | 601 |

A.

Einleitung

A. Einleitung¹

I. Vorüberlegungen

Was haben Auslagerungen und die Raumfahrt gemeinsam? Auf den ersten Blick nicht allzu viel. Jedoch eine elementare Eigenschaft zeichnet beide aus: das Andocken. Wie beim Andocken an der Internationalen Raumstation ISS ist es bei der Auslagerung wichtig, dass die ausgelagerten Aktivitäten und Prozesse weiterhin mit dem Institut respektive dem Internen Kontrollsystem verbunden sind. 1

Diesem Andock-Prozess wird auch mit der 3. Auflage wieder angemessen Rechnung getragen, um sich umfassend mit den Anforderungen und deren Umsetzung in der Praxis zu befassen. Wie schon in den Voraufgaben wird sodann deutlich, dass die Auslagerung allein keinen Selbstzweck verfolgt, sondern mittlerweile insbesondere im IT-Bereich für das Betreiben des Bankgeschäfts von elementarer Bedeutung ist. Diesem symbiotischen Zusammenhang folgend ist die Einbeziehung von Auslagerungen in das Interne Kontrollsystem geboten. Nicht nur die internen (Geschäfts-)Prozesse bedürfen einer regelmäßigen und angemessenen Überwachung, sondern auch die ausgelagerten Komponenten. Diese Sichtweise wird auch seit Jahren von qualitativen Anforderungen der Regulierungsbehörden, insbesondere der Bankenaufsicht, gefordert und findet sich in den einschlägigen Regelungen. Hierzu zählen neben der EU-Verordnung DORA² (Digital Operational Resilience Act) für den gesamten Finanzsektor auch die entsprechenden EBA-Leitlinien zur Auslagerung³, sowie die jeweiligen sektorspezifischen nationalen Regelungen, im Bankensektor z. B. in den MaRisk⁴ sowie in Teilen spezifischer in den BAIT⁵. 2

Idealerweise fängt die Auslagerungsthematik bereits in der Strategie mit der Definition von klaren überprüfbaren Aussagen an und leitet über den Informatrisikomanagementprozess zum Auslagerungsmanagementprozess über. 3

1 Die nachfolgenden Interpretationen und Meinungen sind ausschließlich persönliche Auffassungen des Autors und stellen keine offizielle Meinungsäußerung der Deutschen Bundesbank dar.

2 Vgl. *EU* (2022): Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act) vom 14.12.2022, Anwendung ab dem 17.01.2025.

3 Vgl. *EBA* (2019).

4 Vgl. *BaFin* (2024a).

5 Vgl. *BaFin* (2021b).

- 4 In der Praxis ist vor allem die Diskussion über die Hierarchie von Schutzzielen von Relevanz. Es ist unstrittig, dass die Informationstechnologie möglichst jederzeit zur Verfügung stehen sollte. Um dieses Schutzziel zu erreichen, haben mithin viele Institute oder deren Auslagerungsmandanten erhebliche Ressourcen in die IT-Infrastruktur investiert. Derjenige, der an dieser Stelle die Diskussion mit dem Verweis abbricht, alles getan zu haben, droht zu ignorieren, dass sich die angemessene Steuerung und Überwachung operationeller Risiken im IT-Bereich nicht allein mit dem Schutzziel Verfügbarkeit erreichen lässt. Mindestens ebenso wichtig sind die weiteren Schutzziele Integrität, Authentizität und Vertraulichkeit der Daten. Was nützt es einem Institut, auf verfügbaren Systemen von Dienstleistern zu arbeiten, wenn gleichzeitig nicht sichergestellt werden kann, dass die Veränderbarkeit von Daten in einem fest vordefinierten Umfeld erfolgt? Um dies zu vermeiden, müssen Schreib- (Integrität, Authentizität) und Leserechte (Vertraulichkeit) an Daten einem kontrollierten Benutzerberechtigungsvergabeprozess anhand eines Sollkonzeptes folgen. Die anschließende Kontrolle in Form der Rezertifizierung der eingeräumten Benutzerberechtigungen ist eine Kernkomponente des Internen Kontrollsystems im IT-Bereich sowohl im Institut als auch bei ausgelagerten Aktivitäten.
- 5 Gleichwohl wie gut die einzelnen Schutzziele verfolgt und erreicht werden, kann eine 100%ige Sicherheit – auch unter betriebswirtschaftlichen Aspekten – weder vom Institut noch vom Dienstleister erwartet werden, so dass die Geschäftsleitung eines Instituts permanent mit der Steuerung der verbleibenden operationellen (Rest-)Risiken – auch beim Dienstleister – konfrontiert ist.

II. Aufbau des Werkes

- 6 In den folgenden Buchabschnitten möchten die Autoren Ihnen Anregungen für verschiedene Ausprägungen des Internen Kontrollsystem für den Auslagerungsbereich aufzeigen, welche nach aufsichtlichem Verständnis ebenfalls geboten sind.
- 7 Die Anforderungen sind dem Grunde nach selbstverständlich auf jedes Auslagerungsverhältnis übertragbar, jedoch jeweils immer vor dem Hintergrund der Angemessenheit zu beurteilen. Wichtig ist in diesem Zusammenhang zudem der gesunde Menschenverstand. Hierzu ein vereinfachtes Beispiel: Während von einem IT-Mehrmandantendienstleister eine vierteljährliche Risikoberichterstattung verlangt werden kann, ist eine analoge Forderungsübertragung auf Werttransportunternehmen utopisch. In diesen Fällen müssen andere geeignete

Instrumente angewandt werden, um sicherzustellen, dass Veränderungen in der Risikostruktur spätestens nach einem Quartal deutlich werden.

Das vorliegende Buch beginnt zunächst mit einer Beschäftigung mit dem Thema Auslagerung aus der bankaufsichtlichen Perspektive im **Kapitel B** und stellt zentrale Aspekte eines angemessenen Risikomanagements im Umgang mit Auslagerungen dar. Eine Vielzahl von praxisrelevanten Hinweisen bietet dem Leser die Möglichkeit, Fallstricke und wiederkehrende Schwäche zu erkennen und nachhaltig auszuschließen. Zudem wird auf die Chancen und Risiken durch die DORA-Verordnung eingegangen. 8

Anschließend widmet sich das **Kapitel C** dem Thema der Risikoanalyse von Auslagerungen. Verbunden ist diese Thematik immer mit der Frage nach Wesentlichkeit der Auslagerung. In diesem Abschnitt erhalten Sie wertvolle Hinweise zur praktischen Umsetzung und Implementierung von Schnittstellen zwischen den einzelnen Prozessschritten und/oder beteiligten Organisationseinheiten. Gegenüber der Voraufgabe wurde der Abschnitt um die spezifischen Anforderungen an Signifikante Institute (sog. SIs) erweitert, um zum einen den erhöhten Anforderungen an diese Klasse von Instituten Rechnung zu tragen und zum anderen die Anwendung des Proportionalitätsgedankens noch stärker als bisher aufzuzeigen. 9

In **Kapitel D** erfolgt die umfassende Auseinandersetzung mit dem Themenschwerpunkt DORA. In diesem Kapitel werden die nunmehr finanzmarktweit geltenden Regelungen an die Informationstechnologie aufbereitet und mögliche Handlungsoptionen dargelegt. Insbesondere für IT-Auslagerungen erfordern die neuen Anforderungen ein deutlich breiteres Befassungsspektrum als dies bisher in der Bankpraxis flächendeckend vorzufinden war. 10

Anschließend erfolgt in **Kapitel E** die Betrachtung des Aufbaus einer angemessenen Dienstleister-Steuerung. Hierzu wird zunächst der rechtliche Rahmen umfassend abgesteckt und auf das erforderliche Zusammenspiel der Funktionen in den Instituten abgestellt. Im Anschluss wird anhand von Praxisbeiträgen der Aufbau einer Auslagerungssteuerung einer Bank und einer Versicherung vorgestellt und vertieft. 11

Das **Kapitel F** beschäftigt sich vorrangig mit dem Thema der Auslagerbarkeit von zentralen Komponenten des Risikomanagements. Gerade besondere Funktionen, wie die Risikocontrolling- und Compliance-Funktion sowie die Interne Revision, sind nicht uneingeschränkt auslagerbar. Jedoch gerade vor dem Hintergrund der bankaufsichtlich propagierten »Doppelten Proportionalität« 12

ergeben sich nutzbare Spielräume. Interessant wird es insbesondere bei der Begrenzung dieser Spielräume.

- 13 Eine Besonderheit im Bereich der Auslagerungen stellt die Übertragung der Funktion des IT-Sicherheitsbeauftragten dar und wird daher im **Kapitel G** entsprechend gewürdigt. Dabei wird insbesondere die Sensibilität dieser Auslagerungsoption aufgezeigt.
- 14 Das **Kapitel H** setzt sich mit dem Thema der Integration von ausgelagerten Aktivitäten in dem Internen Kontrollsystem auseinander. Es erfolgt eine umfassende Aufbereitung der Schnittstellen im Internen Kontrollsystem über die alleinigen Auslagerungsanforderungen des AT 9 der MaRisk hinaus.
- 15 Welche Aktivitäten zur Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen vorgenommen werden sollte, ist Bestandteil des **Kapitels I**, welches sich praxisorientiert mit den entsprechenden Kontrollhandlungen auseinandersetzt und entsprechende Handlungsoptionen vorbereitet.
- 16 Grundsätzlich besteht die Erwartung, dass beim Dienstleister »alles rund läuft«. Da dies – wie im eigenen Haus – nicht immer 100%ig klappt, setzt sich das folgende **Kapitel J** mit dem Thema Handlungsoptionen und Notfallpläne intensiv auseinander und stellt verschiedene Alternativen zum Umgang vor.
- 17 Ein zentrales Thema im Umgang mit Auslagerungen besteht in der Weiterverlagerung. Gerade solche Auslagerungsketten begünstigen das Eintreten einer »Aus den Augen, aus dem Sinn«-Mentalität. Hier gilt es jedoch vorzubeugen und sich den Herausforderungen zu stellen. Im **Kapitel K** erhalten Sie dazu umfangreiche Informationen zum erfolgreichen Umgang mit Weiterverlagerungen.
- 18 Die Aspekte der Steuerung und Überwachung von Dienstleistern stehen im Vordergrund des **Kapitels L**, welches sich mit der Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen beim Dienstleister auseinandersetzt. Auch an dieser Stelle wird dem Proportionalitätsgedanken Rechnung getragen, sodass jeweils ein Beitrag mit dem Schwerpunkt SI und ein Beitrag mit dem Schwerpunkt LSI⁶ Eingang in das Werk gefunden haben.

6 LSI = less significant institution, weniger bedeutendes Institut im Sinne des SSM-Verständnisses der europäischen Bankenaufsicht.

Neben den bisherigen Themen des Internen Kontrollsystems kommt der Revi- 19
sionstätigkeit als zweites Standbein der Internen Kontrollverfahren eine heraus-
gehobene Position zu. An welchen Stellen die Revision tätig werden soll, ist
Bestandteil des **Kapitels M**. Das Vorgehen und Zusammenwirken im Risiko-
management werden umfassend erläutert und eine Vielzahl an praktischen Hil-
festellungen gegeben.

Zum Abschluss dieses Werkes wird im **Kapitel N** noch auf den aufsichtlichen 20
Umgang mit Auslagerungen im Bereich der Kapitalfestsetzung und im Rahmen
von Bankgeschäftlichen Prüfungen eingegangen.

Insgesamt handelt es sich – auch in der 3. Auflage – um ein Praktikerhandbuch, 21
welches die Lösung der Aufgaben voranstellt. Teilweise ist es jedoch erforder-
lich, zunächst eine gewisse Problemsensibilität zu entfalten. Aber wenn Sie es
schon bis hierher geschafft haben, dann sollte Problemsensibilität nicht unbe-
dingt eine fehlende Eigenschaft sein.

Ich wünsche Ihnen viel Spaß beim Lesen und die erfolgreiche Verprobung mit 22
Ihren eigenen institutsinternen Vorgehensweisen und Verfahren.

Glück Auf!

B.

Begriffsbestimmung und Abgrenzungstatbestand

B. Begriffsbestimmung und Abgrenzungstatbestand⁷

I. Bedeutung der Auslagerung im Internen Kontrollsystem

1. Vorbemerkungen

Das folgende Kapitel fokussiert sich zunächst auf die allgemeinen Anforderungen an Auslagerungsverhältnisse aus Sicht der MaRisk und somit aus Sicht einer Bank, kann aber im Wesentlichen auf andere Teilnehmer des Finanzmarktes übertragen werden. Spezifische Anforderungen im Informationstechnologie-Bereich werden entsprechend ausgeführt. Mit Anwendung von DORA ab dem 25.01.2025 gelten im IT-Auslagerungsbereich zusätzliche Anforderungen. Zu deren detaillierten Handhabung wird auf das Kapitel D verwiesen. Gleichwohl plant die Aufsicht gemäß dem Anschreiben zur letzten MaRisk-Novelle vom 29.05.2024⁸, die die aktuell gültigen bankaufsichtlichen bzw. zahlungsdiensteaufsichtlichen/versicherungsaufsichtlichen/kapitalverwaltungsaufsichtlichen Anforderungen an die IT (BAIT, ZAIT, VAIT und KAIT) aufzuheben, um eine Doppelregulierung zu vermeiden. Zudem ist zu beachten, dass der Text der DORA-Verordnung noch um weitere Spezifikationen der EBA (sog. ITS – Implementierungsstandards sowie RTS – Regulatory Technical Standards) erweitert werden wird. 23

Aufgrund des finanzsektorübergreifenden Charakters der DORA sind alle drei europäischen Aufsichtsbehörden (EBA, EIOPA, ESMA)⁹ gemeinsam beauftragt worden, Entwürfe für die technischen Regulierungs- und Durchführungsstandards der EU-Kommission vorzulegen. RTS und ITS, die bisher als finale Berichte der Entwürfe durch die ESAs vorliegen, werden im weiteren Prozess von der Europäischen Kommission noch angenommen und geprüft, bevor sie im Amtsblatt der EU veröffentlicht werden. 24

7 Autor: *Henning Riediger*. Die nachfolgenden Interpretationen und Meinungen sind ausschließlich persönliche Auffassungen des Autors und stellen keine offizielle Meinungsäußerung der Deutschen Bundesbank dar.

8 Vgl. *BaFin* (2024a), Anschreiben sowie die erfolgte Umsetzung im Januar 2025, vgl. *BaFin* (2025), mit der Aufhebung von BAIT, KAIT und ZAIT mit Ablauf des 16.01.2025 und für die BAIT mit der Änderung des Anwenderkreises: Banken bzw. Kreditinstitute, die DORA umsetzen müssen, gelten die MaRisk mit Ablauf des 16.01.2025 nicht mehr, anderenfalls gilt die Aufhebung der BAIT zum 31.12.2026.

9 EBA = Europäische Bankenaufsichtsbehörde, EIOPA = Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, ESMA = Europäische Wertpapier- und Marktaufsichtsbehörde.

25 Die MaRisk fordern den Aufbau Interner Kontrollverfahren, welche sich wiederum aus dem Internen Kontrollsystem und der Internen Revision zusammensetzen (vgl. Abbildung B-1). Die Aufgabe des Internen Kontrollsystems ist de facto die Kontrolle der eingerichteten Prozesse und Überwachungsaufgaben. Die Kontrollen dienen mithin dem Ziel, Fehler, Schwachstellen und Mängel im Prozess transparent zu machen und dem Management die Möglichkeit zu bieten, korrigierend einzugreifen. Hingegen sollten die Aufgaben der Internen Revision sich darauf konzentrieren, zu beurteilen, ob das eingerichtete Interne Kontrollsystem funktionsfähig ist. Losgelöst von der idealtypischen Aufgabenverteilung ist in der Praxis häufig festzustellen, dass die eigentlich im Internen Kontrollsystem zu erwartenden Kontrollhandlungen durch die Interne Revision wahrgenommen werden. Derartige Funktionstrennungsverstöße führen im Ergebnis zu einer Einschränkung der Unabhängigkeit der Internen Revision, da die entsprechenden Prüfungshandlungen in der Folge entweder nicht mehr durchgeführt werden oder es aber zu einer nicht zweckmäßigen Überprüfung der eigenen Tätigkeiten kommt.

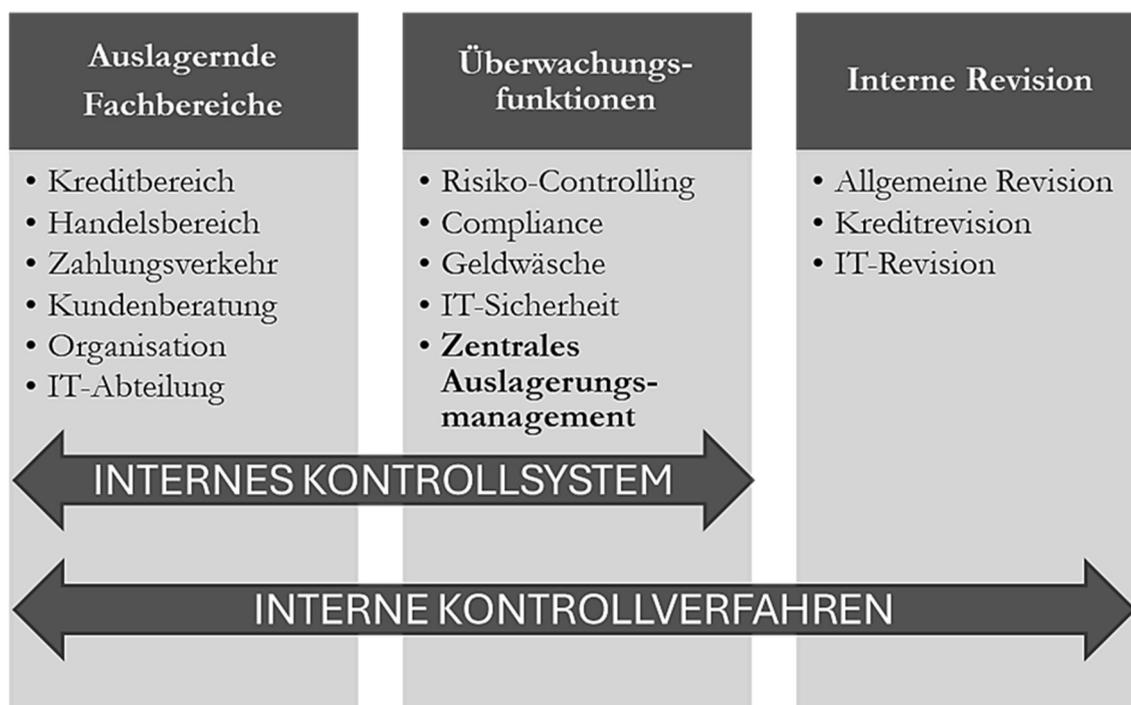


Abbildung B-1: Konzept der drei Verteidigungslinien bei Auslagerungen.¹⁰

26 Die Fachbereiche, welche das »Tagesgeschäft« mit den integrierten Kontrollen (z. B. Vier-Augen-Prinzip) abwickeln, stellen nach diesem Konzept die erste

¹⁰ Quelle: Eigene Darstellung.