BROCKHAUS AG

# ERLANGUNG BAIT UND MaRisk COMPLIANCE

UNTERSTÜTZUNG BEI DER UMSETZUNG REGULATORISCHER ANFORDERUNGEN

## AUSGANGSSITUATION

Unser Kunde ist ein erfolgreiches Startup-Unternehmen in der Fintech-Branche, welches seit der Gründung 2018 seinen Fokus auf Wachstum und eine schnelle Reaktionsfähigkeit auf Marktveränderungen setzt.

Mit dem Gesetz zur Umsetzung der Änderungsrichtlinie zur vierten EU-Geldwäscherichtlinie vom 19.12.2019 benötigte unser Kunde eine Erlaubnis der BaFin für den Geschäftsbetrieb. Um die temporäre Erlaubnis in der Übergangsfrist in eine permanente Erlaubnis umzuwandeln, war das Unternehmen dazu gezwungen, die regulatorischen Anforderungen nach BAIT und MaRisk zu erfüllen. Im Fokus standen insbesondere noch nicht erfüllte Anforderungen an die Bereiche (IT-)Governance, Informationssicherheit, Identitäts- und Rechtemanagement, IT-Projekte und Anwendungsentwicklung, IT-Betrieb, das IT-Notfallmanagement sowie das Risikocontrolling.

## VORGEHEN

Bei der Erarbeitung der Prozesse in der ersten Projektphase hat das Projektteam im ersten Schritt Prozessinterviews mit den Fachbereichen durchgeführt. Im zweiten Schritt wurden die Ergebnisse mittels PlantUML in Aktivitätsdiagramme überführt. Abschließend hat unser Team in der letzten Stufe aus den Diagrammen detaillierte Prozessbeschreibungen abgeleitet. Ein konstanter Austausch mit den Fachbereichen und die Hinweise unserer Berater*innen zu fehlenden Prozessen sowie zu Prozessoptimierungen waren dabei von entscheidender Bedeutung. Parallel zur Erarbeitung der Prozesse unterstützte das Beraterteam beim Aufbau des Risikomanagements durch den Aufbau einer Risikomatrix für operationelle Risiken sowie bei der Ableitung von Prozessrisiken aus den Prozessbeschreibungen und der anschließenden Überführung in die Riskomatrix.

In der zweiten Projektphase wurden die Rückmeldungen der BaFin sowie eines externen Auditors auf Basis des eingereichten Erlaubnisantrages gemeinsam mit dem Kunden gesichtet und in konkrete Aktivitäten überführt. Auf Basis dieser Aktivitäten hat unser Team die folgenden Projektaufgaben übernommen:

Es hat fünf Workstreams abgeleitet und diese in vier Projekte aufgeteilt: Erarbeitung eines Informationsverbundes, Einführung eines Identity Access Managements, Einführung eines Security Operations Centers, Optimierung des IT-Qualitätsmanagements.

Diese vier Projekte haben unsere Berater*innen in einem Management-programm mit dem Ziel der Erreichung der BAIT-Compliance gebündelt und hierfür das Programmmanagement übernommen. Konkret war das die fachliche Führung der Projektleiter*innen, das Controlling des Programmfortschritts, das Risikomanagement des Programms sowie das Berichtswesen an das Management. Darüber hinaus haben sie bei der Erstellung der Fortschrittsberichte an die BaFin unterstützt. Das Projekt zur Erarbeitung des Informationsverbundes unterstützte das Projektteam durch die Erfassung detaillierter Informationen zu allen Prozessen unseres Kunden. Dazu gehörten unter anderem Informationen zum Schutzbedarf der im Prozess verarbeiteten Daten sowie Informationen zur Bedeutung der einzelnen Prozesse für die Aufrechterhaltung des Geschäftsbetriebs. Mittels Power BI wurden die Rückmeldungen der Fachbereiche

## FINANZ-DIENSTLEISTUNG

Nach Abschluss des Projektes konnte unser Kunde, ein erfolgreiches Fintech-Unternehmen, die permanente Betriebserlaubnis durch die BaFin erlangen.

Unsere Berater*innen in dem Projekt modellierten zunächst die Prozesse des Unternehmens zur Dokumentation im Organisationshandbuch und dokumentierten dies in Arbeitsanweisungen.

Nachdem das Projektteam hier fachlich und methodisch sowie mittels diverser Prozessverbesserungen überzeugen konnte, wurde es mit dem Aufsetzen und der Leitung eines Programms zur Erreichung der BAIT-Compliance beauftragt.

Darüber hinaus unterstützte das Projektteam beim Aufbau des Risikomanagements im Bereich Operationelles Risiko.

## TECHNOLOGIEN & METHODEN

- **PlantUML**
- **Power BI**
- **Google Workspace**

in einer zentralen Auswertungsdatei konsolidiert und analytisch für den Informationssicherheitsbeauftragen aufbereitet. Das IT-Qualitätsmanagement berieten sie bei der Entwicklung BAIT-konformer Prozesse zum Requirements-Engineering und Testmanagement. Zudem wirkten unsere Berater*innen beim Aufsatz eines regulatorisch konformen Ausbaus des Projekt- und Prozessmanagements fachlich mit und entwickelten in diesem Zuge Zielbilder, Richtlinien, Prozesse und Vorlagen.

## ERGEBNIS

Mit der Umsetzung des Programms konnte ein Großteil der Rückmeldungen der BaFin sowie des externen Auditors zur BAIT-Compliance in optimierte Prozesse überführt werden. Das Risiko für wesentliche Feststellungen bei der Zulassungsüberprüfung für eine permanente Erlaubnis wurde so erheblich reduziert.

Nach unserer erfolgreichen Projektdurchführung konnte die installierte Programm-Governance durch die neu eingestellten internen Mitarbeiter*innen des Unternehmens übernommen und für die verbliebenen Restaktivitäten eigenständig gesteuert werden.

Im Risikomanagement wurde mit den dokumentierten operationellen Risiken eine wesentliche Anforderung aus der MaRisk umgesetzt und die Risiken konnten in die Risikosteuerung sowie das aufsichtsrechtliche Berichtswesen überführt werden.