No time to comply

Wie man den Spagat zwischen agiler Softwareentwicklung und regulatorischen Anforderungen schafft

NEXGEN

NEXGEN Whitepaper
März 2021

Sladjan Seferovic
Tristan Poetzsch

Einführung

Ein Minimal Viable Product (MVP) ist die realisierte Vision eines Produktes oder einer Dienstleistung mit einem zu beziffernden Mehrwert und Kernelement der agilen Arbeitsweise. Ziel eines jeden MVPs ist es, dem Kunden etwas Neues, Schnelleres, Besseres zu bieten und somit eine gewisse Marktdominanz zu erlangen. Allerdings wird man hier oft von der Realität bzw. von der Regulatorik eingeholt und eine Vision wird zu einer Version.

Der Fokus bei moderner und agiler Softwareentwicklung liegt u.a. darauf, möglichst schnell MVPs zu entwickeln und live zu schalten. Unsere Erfahrung zeigt jedoch, dass klassische Banken durch regulatorische Auflagen daran scheitern und das Messen an den sog. Challenger Banken oder Technologiekonzernen nicht mehr als ein hehrer Anspruch ist. Und genau dieser diametrale auseinanderstrebende Anspruch zwischen Geschwindigkeit und Regulatorik es, der viele agile Transformationen im Bankenumfeld deutlich hinter den Erwartungen zurückbleiben lässt. Daher müssen klassische Banken einen Weg finden, wie sie die Regulatorik und die agile Softwareentwicklung in Einklang bringen können. Häufig erstreckt sich das Denken über agile Methoden und MVPs auf neue Produkte und Prozesse, die von Innovationsabteilungen und Clustern entwickelt werden – was auch der Grund für die explizite Forderung des Regulators an einen Neue-Produkte-Prozess (NPP) ist. Unserer Erfahrung nach aber, ist besonders die Umsetzung von bestehenden Core-Banking Funktionen im agilen Modus die Herausforderung, bei welcher der Spagat nicht nur zwischen Agilität und Compliance, sondern auch der operativen Stabilität und der Entwicklung von MVPs gemacht werden muss – in ebenjenen DevOps Teams, die gerade erst aus der Zusammenführung von RTB (run the bank) und CTB (change the bank) entstanden sind.

Häufig zeigt sich in der Detailbetrachtung, dass das Core Banking selbst nur in wenigen Fällen aktuell compliant ist, und gerade hier eine Neuentwicklung unter voller Compliance-Erfüllung besonders wertvoll wäre – auch für das bestehende Personal, das häufig sowohl ungenügend geschult im agilen Modus als auch von der Masse der regulatorischen Anforderungen schachmatt gesetzt wird. Auf den Punkt bringt das ein Managing Directors einer deutschen Großbank:

„Meine Erfahrungen aus den letzten drei Jahren zeigen, dass eigentlich nie auf ein MVP hingearbeitet wird, ohne die regulatorischen Abteilungen einzubinden. Daher wird selten eine Vollbremsung provoziert.

In der Realität ist der Standardfall, dass die Fachabteilung mit den Fachanforderungen startet und minimal zeitversetzt die notwendigen Schnittstellenabteilungen wie Compliance, Datenschutz, Legal, etc. eingebunden werden. Diese stellen dann allerdings weitere Anforderungen innerhalb des Entwurfsprozesses. Da in unserem Haus noch nicht wirklich alles zu 100% agil entwickelt wird, steht in der Regel zumindest der Liefertermin bereits fest. Dies bedeutet dann, dass die Art der Lösung modifiziert werden muss, um so den Termin halten zu können.
Sprich: die Ergebnisqualität wird immer schlechter, weil man innerhalb des definierten Zeitraums allen Anforderungen schnellstmöglich und leider nicht bestmöglich gerecht werden muss. Mein Fazit ist, dass man am Ende somit eine fristgerechte Lösung hat, allerdings keine, die der Kunde am Markt kaufen wird.“

Aber woran erkennen Sie, dass das Thema für Sie relevant ist? Die folgenden Leitfragen können Ihnen helfen, sich im Thema zu orientieren:

1. Ich kann eine Compliance-Anfrage, welche Regulierungen für dieses MVP relevant sind, nicht beantworten.

2. Eine Abstimmung mit Compliance führt immer zu noch mehr Folgemeetings, ohne dass Freigaben erwirkt werden können.

3. Es ist unklar, mit welchen Personen in Compliance ich sprechen muss, ohne es sofort eskalieren zu müssen.

4. Bei Softwareeinführungen implementiere ich ab und zu mehr Funktionen, als ich offiziell angebe.

5. Mein MVP wird immer kleiner als ursprünglich geplant – mein Kunde wird damit nicht zufrieden sein!

Was ist agiles Projektmanagement?

Im Gegensatz zum klassischen Projektmanagement ist die agile Philosophie, dass Timelines und Aufwandsschätzungen von Anfang an gar nicht seriös geplant werden können und sich die funktionalen Anforderungen sowohl in ihrer Priorität als auch in ihrer Natur völlig verändern können. Deswegen wird in kurzen Zyklen (= Sprints, etwa zwei Wochen) gearbeitet und flexibel priorisiert, um den maximalen Wert mit den verfügbaren Ressourcen zu ermöglichen.

Welche Regulierungen gilt es zu berücksichtigen?

Die von der BaFin herausgegebenen Mindestanforderungen an das Risikomanagement (MaRisk) von 2017 spezifizieren die europaweiten Anforderungen für deutsche Banken. So wird darin unter anderem geregelt, welche Mitarbeiter welche Zugriffe erhalten dürfen und wie neue Produkte inklusive deren IT-Komponenten eingeführt werden müssen (NPP). Weiter spezifiziert ist dies in der Bankenaufsichtlichen Anforderungen an die IT (BAIT) von 2018, welche sich momentan in der nächsten Konsultation befinden. Dies hat besonders Auswirkungen auf den Prozess der Neu- und Weiterentwicklung von IT-Komponenten.

Mit der Datenschutzgrundverordnung (DSGVO) von 2018 wird geregelt, dass Kundendaten grundsätzlich nur aus besonderem Grund gespeichert werden dürfen und ansonsten gelöscht werden müssen – was u.a. die Nutzung von Daten im Rahmen von MVPs betrifft.

Zusätzlich müssen lokale Regulierungen für die Know-Your-Customer (KYC) Richtlinien eingehalten werden, vor allem zur Vorbeugung von Geldwäsche und Terrorismusfinanzierung. In Europa gilt hier die Markets in Financial Instruments Directive (MiFID), in den USA die Regelungen des Dodd-Frank Acts. Hier muss insbesondere bei neuen Produkten geprüft werden, ob das MVP bei Kunden bereits alle wichtigen Informationen abfragt.

Im Bezug auf die Risikominimierung im außerbörslichen Handel gilt die European Markets Infrastructure Regulation (EMIR), wobei für MVPs vor allem wichtig ist, zu klären, dass Trading-Reportingpflichten erfüllt werden.

Auch spezifischere Reportings wie das statistische Reporting gemäß dem Money Market Statistical Reporting (MMSR), Aktionärsrichtlinien mit dem Shareholder Rights Directive II (SRD II) und settlementorientierte Richtlinien wie Central Securities Depositories Regulation (CSDR) sind in relevanten Fällen zu berücksichtigen.

„Und genau dieser diametrale auseinanderstrebende Anspruch ist, was viele agile Transformationen im Bankenumfeld deutlich hinter den Erwartungen zurückbleiben lässt“

- Tristan Pötzsch

Experten im Interview

Daniel Back
Product Owner bei Berenberg

Wie erlebst du die agile Transformation bei euch im Haus, insbesondere in der Interaktion von Fach und Compliance-Funktionen?

Daniel: *„Im Vordergrund für uns steht eine exzellente Kundenerfahrung. Daher setzen wir nicht immer auf klassische MVPs, sondern versuchen, bereits sehr reife IT mit wenig Fehlerpotential für unsere Kunden bereitzustellen. In unserer Entwicklung selbst arbeiten wir aber stark orientiert an den agilen Werten. Bei uns ist vor allem ein großer Vorteil, dass Compliance, Audit und Legal trotz ihrer Stabsfunktion sehr darauf eingestellt sind, uns als Delivery Unit im agilen Modus zu unterstützen. Dieses Mindset zeigt sich auch darin, dass unser Audit zum Beispiel mit einem Ticketsystem arbeitet.“*

Was ist dein Erfolgsrezept als Product Owner, um Compliance in den agilen Modus einzubinden?

Daniel: *„Für die Arbeit im agilen Modus legen wir großen Wert auf eine regelmäßige Einbindung von Compliance in den Entstehungsprozess, unter anderem in unseren Sprint Planungen. Dort ziehen wir auch soweit möglich die internen Kunden aus dem Fachbereich zusammen, sodass wir als Delivery Unit eine orchestrierende Funktion haben und die Verhandlung zwischen Fach und Compliance moderieren. Durch diese schlanke Organisation ohne viele Schleifen gelingt es uns, die Geschwindigkeit der Software Delivery hoch zu halten, ohne Kompromisse in der Compliance machen zu müssen. Voraussetzung ist aber natürlich eine engmaschige Einbindung von Fach und Compliance, was auf deren Seite eine hohe Verfügbarkeit voraussetzt.*
Insgesamt haben wir mit diesem Vorgehen bisher sehr gute Erfahrungen gemacht, vor allem auch in der Erfüllung von Auflagen wie der BAIT. Die IT-Strategie und Governance geben uns einen Orientierungsrahmen, die Anforderungen an Sicherheit und bspw. auch Benutzerberechtigung klare Vorgaben.“

Die häufigsten Knackpunkte zwischen MVP-Entwicklung und Compliance

Strukturieren lassen sich die Herausforderungen im Spagat zwischen Agilität und Compliance sowohl auf strategischer als auch auf operativer Ebene. Wichtig ist es, beide Perspektiven für eine umfassende Lösung zu betrachten.

Strategisch	Operativ
Unklarheit über Regularien Den Teams, die MVPs bauen, fehlen sowohl die Erfahrung mit Regularien als auch die Vorbilder und Best Practices für den Umgang mit diesen. Dies gilt sowohl innerhalb der eigenen Firma als auch auf dem Markt	Es gibt keine Betroffenheits-checkliste für Use Cases,
	Es gibt keine Leitfäden für die Umsetzung von Regularien
	Es gibt keine Referenz-implementierung, bzw. sind diese nicht transparent genug innerhalb des Unternehmens
IT Governance ist nicht compliant by design An zu vielen Stellen wird Compliance gefordert, aber eine entsprechende Umsetzung wird nicht operativ unterstützt	Softwarekomponenten werden aus dem Internet bezogen und nicht über ein zentrale Repository, wodurch teilweise unsichere und ungeprüfte Softwarebausteine Verwendung finden
	Release Management ist nicht hinreichend darauf geschult, inhaltlich zu prüfen, was live gesetzt wird
	Es gibt keine standardisierten Softwarebausteine für verbreitete Funktionen, die direkt ab Bereitstellung compliant sind, z.B. für Portalfunktionen oder Logging

Strategisch	Operativ
Regulatorische Abteilungen sind nicht auf agilen Modus eingestellt Der schnelle Modus in der Entwicklung passt nicht zum klassischen Selbstverständnis einer Stabsfunktion	Abstimmungen mit regulatorischen Abteilungen erfolgen im Sinne des klassischen Projektmanagements am Anfang des Projektes, eine Nachschärfung im agilen Sinne erfolgt selten
	Prozessuale Anforderungen wie die Einhaltung von Teststufen werden nicht geprüft, da die Compliance die Prozesse der Softwareentwicklung nicht genügend kennt
	Risikobewertungen und notwendige Freigaben von Compliance-Funktionen werden nicht schnell genug bereitgestellt
Abkürzungen Durch die Forderung von schnellen Entwicklungszyklen werden im Zweifel Compliance-Einbußen hingenommen	Entwickler erhalten im Sinne des DevOps Gedanken produktionsnahe Zugriffe, die sie nicht haben dürften (u.a. auf Datenbanken, Serverfunktionen und Logdateien)
	Virtuelle Maschinen werden auf falschen Hypervisoren aufgebaut, u.a. weil es gerade in die Kapazitätsplanung passt
	Daten werden häufig nicht nach dem need-to-know Prinzip gehandhabt – so landen unter anderem nicht-anonymisierte Produktionsdaten in Pre-Live Umgebungen

Experten im Interview

Sladjan Seferovic
Managing Partner bei NEXGEN

Als Berater dienst du als Bindeglied zwischen Fach und IT. Wie schaffst du diesen Spagat und legst gleichzeitig Wert auf eine agile Transformation?

Sladjan: *"Für diesen Spagat ist eine gewisse Neugierde an Fach und IT-Themen erforderlich und das große Ganze muss verstanden werden. Diese permanente Weiterbildung und die Abschaffung von Silostrukturen schaffen wir, indem Fach und IT-Experten zusammen in agilen Teams arbeiten und eine gemeinsame Vision haben. So kann der Entwicklungs-prozess schneller gestaltet werden und es kommt nicht zu Compliance Lücken, da diese Herausforderung direkt angegangen wird."*

Welche Herangehensweise und Tipps empfiehlst du, um Compliance agile zu machen?

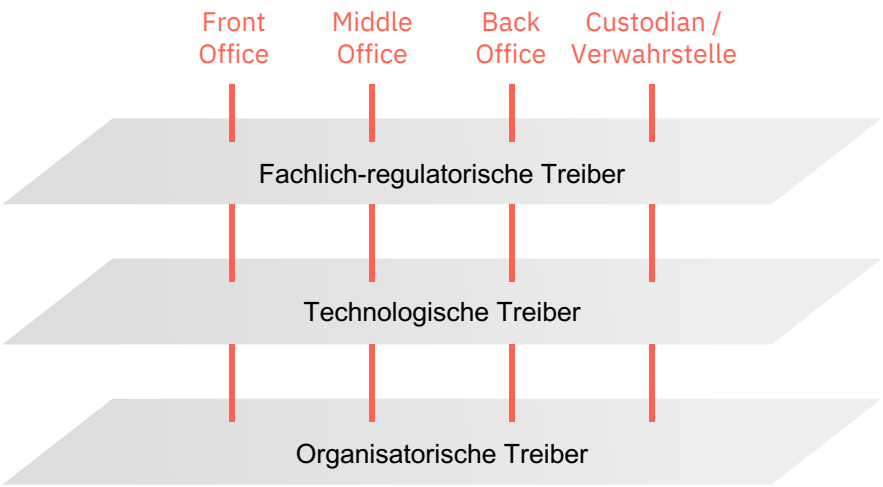
Sladjan: *"In der Vergangenheit waren regulatorische Anforderungen davon gekennzeichnet, dass das ursprünglich Geforderte und das tatsächliche Endergebnis nicht identisch waren. In unseren agilen Teams starten wir sofort mit dem Teil der Regulatorik, welche auf jeden Fall kommt. Im Laufe der Entwicklung können wir durch unsere Flexiblität weitere Anpassungen der Regulatorik stetig mitaufnehmen."*

Gibt es Voraussetzungen für Finanzdienstleister, um den Sprung mit Compliance in den agilen Modus zu schaffen?

Sladjan: *"Die Bereitschaft, agil arbeiten zu wollen, ist essenziell. Für dieses Mindset muss man bereit sein, das Silodenken in den Abteilungen zu reduzieren. Dies schafft man, in dem Compliance Verantwortliche von Beginn an im agilen Team mitarbeiten und den Compliance Aspekt mit in die Produktvision und Sammlung an Anforderungen mitaufnehmen."*

Welche Lösungsansätze helfen, trotz agilen Modus, compliant zu bleiben

Um sowohl im NPP als auch im Core Banking den Wunsch nach Agilität wie auch die Anforderungen des Regulators umzusetzen, strukturieren sich Lösungsmöglichkeiten über den NEXGEN 3 Layer Approach in die Treiber Fach, IT und Organisation, unabhängig vom Fachbereich und der Funktion.



Nicht immer ist es einfach, die Veränderungen in der Organisation direkt so umfassend anzustoßen, dass der Weg Richtung agiler Compliance in großen Schritten gegangen werden kann. Natürlich muss der erste Schritt sein, die Perspektiven der Delivery Unit und Compliance näher zusammenzubringen. Die Möglichkeiten hierzu sind vielfältig: Von der Mitnahme von Compliance-Kollegen in agile Schulungen, über die aktive Einbindung in die Sprint Reviews sind einige Modi möglich. Dort kann sowohl einfach als auch wiederkehrend der Kontakt und das Verständnis intensiviert werden. Ein Regeltermin zum Austausch über aktuelle Herausforderungen hilft. Sinnhaft ist es natürlich, einen festen Ansprechpartner vonseiten der Compliance zu gewinnen, mit dem man den Weg gemeinsam gehen kann, um dann auch größere Änderungen anzustoßen.

Fachliche-regulatorische Treiber

Die Hebelwirkung der regulatorischen Orientierung und Referenzimplementierung für die Delivery Units ist enorm

1. Durch die Erstellung einfacher Checklisten zur einfachen Identifikation und Anwendung relevanter Regularien kann den Software Delivery Units eine Hilfestellung gegeben werden, ob und inwiefern sie von verschiedenen Regularien betroffen sind. Ein Self-Service Tool mit Orientierungsfragen ist hier eine einfache und effektive Lösung.

2. Ein Mapping von Funktionalitäten, Daten, Produkten oder Prozessen auf betroffene Regularien erleichtert den Delivery Units, abzuschätzen, mit welchen Inkrementen sie welche Regularien tangieren und wo entsprechende Compliance-Anforderungen entstehen. So können folgende Funktionalitäten bereits vorher klassifiziert werden:
   - Trade-Aufnahme oder Settlement
   - Produkte wie Foreign Exchange oder Swaps
   - Datenklassen wie personenbezogene Daten oder besonders schützenswerte Kunden
   - Prozesse wie OTC-Handel oder Buy-Ins

3. So können Funktionalitäten wie Trade-Aufnahme oder Settlement, Produkte wie Foreign Exchange oder Swaps, Datenklassen wie personenbezogene Daten oder besonders schützenswerte Kunden und Prozesse wie OTC-Handel oder Buy-Ins bereits vorher klassifiziert werden.

4. Die Stärkung des internen Netzwerkes und die Verbreitung von Referenzimplementierung hilft den Entwicklern nicht nur sich selbst zu orientieren, sondern fördert auch die parallele Weiterentwicklung in den bereits bestehenden Use Cases. Insbesondere ein aktives Monitoring und die Pflege von Kontakten zu Referenzimplementierung durch Compliance kann dazu dienen, anderen Software-Initiativen auf die Sprünge zu helfen und dem Bild der stets fordernden, aber wenig unterstützenden Organisationseinheit, positiv entgegenzuwirken.

5. Die Entwicklung von standardisierten Use Cases (z.B. Änderung von Nutzerdaten, Freigabe von Trades) inklusive einer standardisierten Compliance-Bewertung kann bei der Planung von MVPs und Sprints helfen. Die Kombination von bestimmten Funktionalitäten kann somit auf die tangierten Regularien und den damit verbundenen Aufwand optimiert werden.

Technologische Treiber

Im technologischen Bereich sind Standardisierung und compliance-by-design die wichtigsten Lösungsansätze

1. Die Einführung von Frameworks mit Standardkomponenten und Libraries nimmt Entwicklern nicht nur viel Arbeit ab, sondern sorgt auch für compliance-by-design: Dafür ist ein DSGVO-konformes Nutzermanagement ein gutes Beispiel. Als Referenz dient hier zum Beispiel das Framework JAVA FRAME in der Commerzbank. Baukästen können sogar bis hin zu ganzen Applikationskernels, Boilerplates für WebApps oder vorkonfigurierten Images für einen containerbasierten Betrieb gehen. Auch komplette Stacks wie Apache CloudStack können sinnvoll zum Einsatz kommen.

2. Um Fehler und Risiken bereits im Aufsatz zu verhindern, sind vorkonfigurierte Infrastrukturen, welche bereits standardisiert die relevanten Regulierungen unterstützen, ein sinnvoller Ansatz. Dies betrifft u.a. Konnektivitäten, Zugriffsberechtigungen und Firewalls. Ein zeitgemäßer Ansatz hierzu ist Infrastructur-As-Code (IaC), zum Beispiel mit Terraform.

3. Eine Continuous Integration & Deployment Pipeline für den Einsatz von Software in die Produktion erlaubt schnelle Änderungen und unterstützt somit besonders Hyper-Care im Rahmen eines Releases, ohne dass Entwickler direkt auf Produktionsumgebungen Fehlerbereinigungen anstreben. Somit werden insbesondere von BAIT geforderte Rechtevergaben nicht verletzt und parallel wird auch der allgemeine Prozess zur Softwareeinführung verbessert.

4. Die Bereitstellung von Referenzimplementierungen mit Compliance-Relevanz als Mikroservices (Aufgabenspezifische Codes, welche unabhängig sind und dadurch wiederverwendet werden können) kann dabei unterstützen, doppelte Entwicklungsarbeit zu vermeiden. Insbesondere bei Funktionen, die von vielen Systemen benötigt werden, wie z.B. alternative Identifier zu führen, ist somit vereinfacht und reduziert die potentiellen Fehlerquellen und Compliance-Verletzungen. Auch für fachliche Funktionen wie z.B. im Bereich Transaction Reporting gibt es hier sinnvolle Möglichkeiten.

Organisatorische Treiber

Besonders in der Zusammenarbeit und den Meetingstrukturen gibt es häufig Verbesserungspotentiale mit hoher Wirksamkeit

1. Compliance-by-design ist im Softwareentwicklungsprozess ein Ansatz, in welchem Compliance-Anforderungen bereits im Designprozess des Geschäftsprozesses und der Entwicklung mitgedacht und somit mit möglichst geringem Aufwand erfüllt werden. Compliance-by-design wird ermöglicht, wenn die Delivery Unit kontinuierlich hinsichtlich relevanter Regulatorik fortgebildet wird und somit bestimmte Herausforderungen von Anfang an betrachtet werden kann. Die entsprechende Wissensvermittlung in die Organisation einzuführen, bedarf häufig eines Top-Management gestützten Programmes.

2. Häufig ist es sinnvoll, explizite Compliance Sprints sowohl in der Konzeption als auch in der Implementierung des MVPs durchzuführen. Entsprechende Anforderungen nicht mehr in Konkurrenz zu fachlich-funktionalen Anforderungen umzusetzen, kann Spannungen im Team und zwischen Anforderern entgegenwirken und somit die Delivery Unit entlasten. Je nach Reifegrad der Compliance-Organisation kann auch eine Einbeziehung in die Sprintplanungen regulärer Sprints erfolgen.

3. Die Entwicklung eines standardisierten Prozesses, um Use Cases und IT-Setups einfach und schnell mit einem Risikoscore und/oder einer Compliance-Einschätzung zu versehen, ist ein weiterer organisatorischer Hebel. Insbesondere für die Refinements und Sprint Planungen ist eine schnelle und belastbare Reaktion ein Eckpfeiler für gelungene Implementierungen.

4. Jede Delivery Unit sollte einen fixen Ansprechpartner aus der Compliance haben – so wie es heutzutage auch bereits für die Rolle der Enterprise Architekten gehandhabt wird. So gewinnt nicht nur der persönliche Kontakt und damit häufig die Geschwindigkeit von Klärungen, sondern auch die Qualität von fachlichen Entscheidungen. Postboxen und Verteiler halten Anfragen zwar flexibel für die Compliance, sind aber häufig ein Bottleneck für die schnelle und agile Welt der Softwareentwicklung.

Interessiert an mehr?
Ihre Ansprechpartner:

Sladjan Seferovic

Managing Partner

sladjan.seferovic@nexgenbc.com

Tristan Pötzsch

Manager

tristan.poetzsch@nexgenbc.com

NEXGEN

NEXGEN Business Consultants GmbH
Grüneburgweg101
60323 Frankfurt am Main