Grey Swan

Neue Ordnung

Programm Management unter neuen regulatorischen Anforderungen

Leon Kuhlmann
Julius Düwel
Pauline Schmidt
Tamino Müller

Grey Swan Management AG
April 2024
Whitepaper

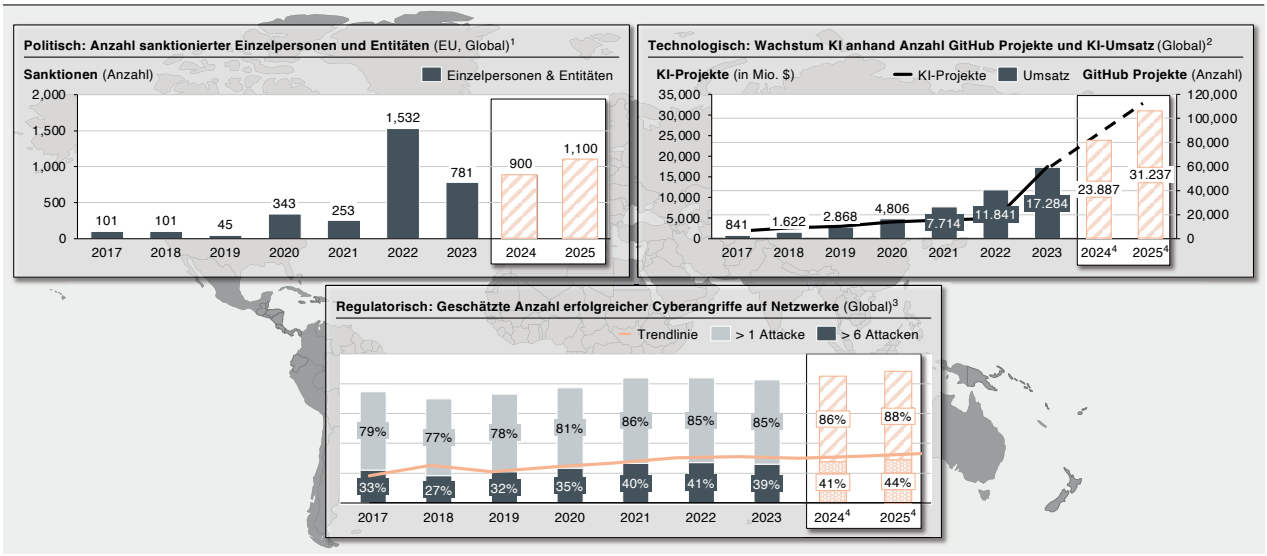
Management Summary

- Aktuell sehen sich Unternehmen vielfältigen Herausforderungen gegenübergestellt, die massive Auswirkung auf Strategien sowie die Geschäftsfähigkeit in sich verändernden Märkten aufzeigen: politische, technologische und regulatorische.
- Aufsichtsrechtliche Entwicklungen in Europa verschärfen regulatorische Herausforderungen für Unternehmen und Einrichtungen der kritischen Infrastruktur (KRITIS), durch übergeordnete und teils industrieunabhängige regulatorische Standards wie Netzwerk-Informationssicherheitsrichtlinie 2.0 (NIS2), Critical-Entities-Resilience-Richtlinie (CER), Cyber-Resilience-Act (CRA), Datenschutz-Grundverordnung (DSGVO) und der Verordnung zur Digitalen Operativen Resilienz (DORA).
- Die Berücksichtigung dieser Gesetze im Geschäftsverkehr stellt Unternehmen regelmässig vor grosse Hürden u.a. in der regulatorisch konfliktfreien Gestaltung von Cross-Market-Abhängigkeiten bei operativem Geschäft in mehreren Ländern, bei politischen Unwägbarkeiten, der Vermeidung von „Overspending“ für Compliance und der Frequenz in der Veröffentlichung neuer oder Veränderung bestehender Gesetze und deren Umsetzung.
- Um regulatorisch motivierte Programme oder Audits im Ergebnis positiv zu beeinflussen, unterstützt ein Framework aus Gap-Analyse, Audit (inkl. Vorbereitung und Durchführung) sowie Mängelbeseitigung durch Präparation, Planung und Umsetzung.
- Erfolge in diesen Vorhaben werden ausschlaggebend durch drei Aspekte beeinflusst: dem Vorhandensein von methodischer Kompetenz, der Verfügbarkeit von und Fähigkeit zum Umgang mit Tools sowie der Verfügbarkeit von Experten (Subject Matter Experts) für fachspezifische Themen.
- Mängelbeseitigungsprogramme im Auditprozess bergen Besonderheiten und sollten eine angemessene Governance, detaillierte Mängelbeseitigungsplanung, strukturierte Abnahmeprozesse für Evidenzen, faktenbasierte Berichterstattung, Überprüfung von Massnahmen nach Test of Design (ToD), Test of Implementation (ToI) und Test of Effectiveness (ToE) und Ende-zu-Ende-Lieferprozesse beinhalten.
- Die Allokation von Projektmanagement-Kapazitäten kann für Programme, inklusive regulatorischen, von Organisationen in drei Modellen gestaltetet werden: Insourcing, vollständiges Outsourcing mit RAID-Ansatz (Redundant Arrays of Independent Disks; im Sinne von Nutzung verschiedener Service Provider zur Risikominimierung) oder Hybrid im Delivery Modell.

Politische, technologische und regulatorische Herausforderungen für Unternehmen

Unternehmen in diversen Industrien stehen angesichts der Entwicklungen im Markt aktuell vor Herausforderungen die politisch, technologisch oder regulatorisch geprägt sind. Bei oberflächlichem Blick auf politische Herausforderungen sind Bussgelder durch Gesetzesverstösse, z.B. DSGVO, eine offensichtliche und finanziell herausfordernde Konsequenz für Unternehmen. Die technologische Entwicklung zeigt die erwartbare rapide Akzeptanz der nächsten Technologie-Schritte, wie künstlicher Intelligenz, somit Veränderung des Kundenverhaltens als auch in spezifischen Ökosystemen der Unternehmen. Die Regulatorik betrachtend, stellt sich die Frage, wie schützenswerte, kritische Infrastrukturen KRITIS (im Entwurf zum IT-SiG 3.0 wird der KRITIS-Bereich erweitert zu „Betreiber kritischer Anlagen, besonders wichtige und wichtige Einrichtungen“ und nachfolgend „KRITIS“ und „kritische Infrastruktur“ genannt) und die darin verarbeiteten Kundendaten gemäss den regulatorischen Vorgaben vor der zunehmenden Anzahl (erfolgreicher) Angriffe besser abgeschirmt werden können (Abbildung 1).

Entwicklung und Quantifizierung der politischen, technologischen und regulatorischen Herausforderungen



1: Data Europa I 2: GitHub I 3: CyberEdge I 4: Grey Swan Research Institute - Berechnung einer Prognose auf Basis von vorhandenen Daten

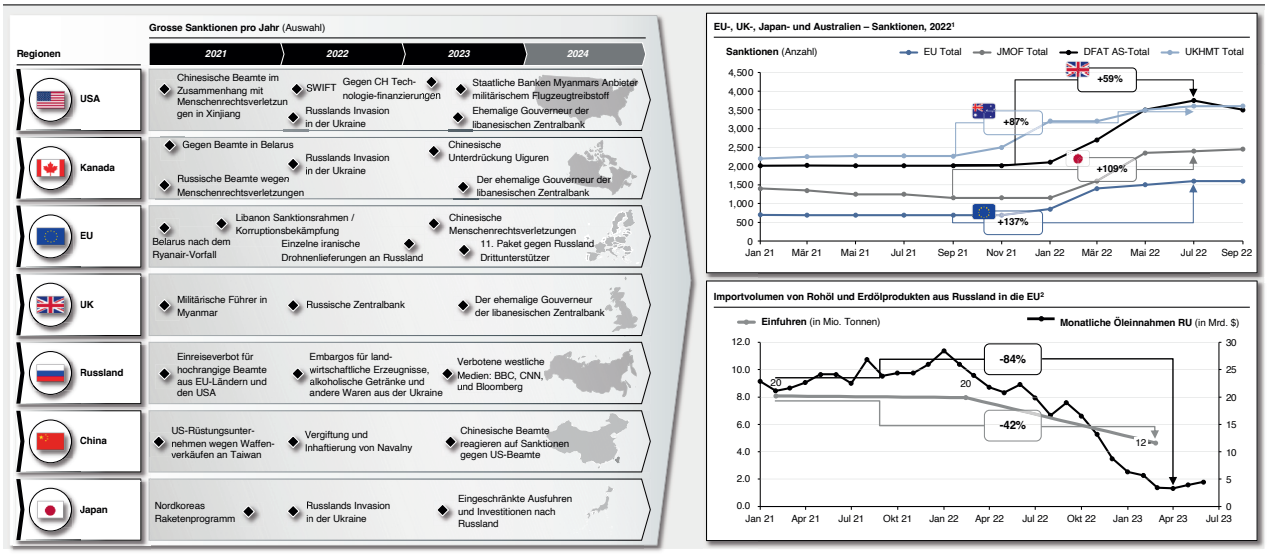
Abbildung 1: Politische, technologische und regulatorische Herausforderungen

Politische Herausforderungen entstehen für Unternehmen bei Verstössen gegen Gesetze oder nicht von der Politik unterstützte Geschäftspraktiken.

- Erstens durch restriktive Massnahmen bzw. „Sanktionen“, die als wichtiges Instrument der Aussen- und Sicherheitspolitik von Regierungen weltweit genutzt werden. Sie richten sich gegen Regierungen von Nicht-EU-Mitgliedstaaten oder gegen Unternehmen, die die sanktionierte Politik unterstützen (Abbildung 2). Ebenso gegen Gruppen oder Vereinigungen und Einzelpersonen, für die gleiche Annahmen gelten[1]. Die Anzahl der von der Europäischen Union ausgesprochenen Sanktionen gegen Einzelpersonen und Entitäten stieg von 101 im Jahr 2017 auf 1.532 im Jahr 2022, was einem Anstieg von 1.417% entspricht[2].

- Zweitens aus der Lieferketten-Optimierung und -Organisation, genannt EU-Lieferkettenrichtlinien 2022 (CSDDD)[3], welche Unternehmen zwingt, standort- und länderübergreifend eine rechtssichere und Compliance-konforme Umsetzung von gesetzlichen Anforderungen sicherzustellen. Auch die Überprüfung von Zulieferern auf die Einhaltung menschenrechtlicher als auch umweltbezogener Standards ist verpflichtend angeordnet. Ebenso die Einflussnahme auf Optimierung von Nachhaltigkeitsanforderungen in der Lieferkettenorganisation. Diese Anforderungen reichen weit über die bestehenden Rechtsvorschriften auf nationaler Ebene hinaus, sodass bei Nicht-Einhaltung politische Folgen wie zivilrechtliche Haftung für Schäden, die aus Unterlassungen resultieren, sowie erhebliche Bussgelder, deren Höhe von der Schwere des Verstosses abhängt, drohen.

Überblick über die wichtigsten Sanktionen und Folgen einzelner Handlungen



Quelle: Grey Swan Research Institute I 1: Statista, Refinitiv I 2: Statistisches Bundesamt

Abbildung 2: Sanktionsentwicklungen, Vorkommnisse und Auswirkungen

- Ein dritter Aspekt, den es aus politischer Perspektive von Unternehmen zu berücksichtigen gilt und der sicherheitspolitische Relevanz hat, ist die Verwendung von amerikanischen und chinesischen Technologie-Stacks beispielsweise in der Telekommunikationsinfrastruktur (5G) oder auch in IT-Architekturen (Cloud) von Banken und Versicherungen. Aber nicht nur dort. Hier ist die Einhaltung von nationalen Vorgaben für die Nutzung von ausländischen Technologien unter anderem in kritischen Infrastrukturen massgeblich. Der chinesische Netzausrüster Huawei ist hervorzuheben, der für die Europäische Union als „Hochrisiko-Anbieter" gilt und nun aus Deutschlands 5G Infrastruktur verbannt werden soll. Im Gegenzug sind U.S.-amerikanische Technologie-Provider in den BRICS-Staaten aufgrund günstigerer Preise bei gleicher oder teilweise besserer Funktionalität sowie aus Sanktionsfolgegründen ausgelistet, sodass die Proliferation chinesischer Technologien in den BRICS-Staaten zunimmt (siehe Whitepaper „The Dark Knight Rises», Grey Swan 2024).

Mithin ist die digitale Wettbewerbsfähigkeit als Ergebnis des Umgangs mit technologischen Herausforderungen sowie die erfolgreiche Adaption von sich durchsetzenden Technologien erfolgskritisch.

- Die schnellere Verbreitung von Künstlicher Intelligenz als individualisiertes Werkzeug beispielsweise in der Kundenkommunikation in Form von Chatbots, Sprachunterstützung oder Assistenz weist die Richtung. Ebenso werden in der Produktion Daten Event-getrieben erhoben als auch weitgehend automatisiert analysiert[4].

- Zudem hat die Anwendung von Cloud Computing mittlerweile ihren Weg in fast allen grösseren Unternehmen gefunden. Primär verwendete Cloud-Module sind Infrastructure as a Service (IaaS), Platform as a Service (PaaS), und Software as a Service (SaaS). Die Prognose von Gartner, dass 70% der Unternehmen bis 2027 Enterprise Cloud-Lösungen nutzen werden, macht deutlich, dass Cloud-Computing kein Trend, sondern eine strategische Geschäftsentscheidung[5] ist.

- Weitere Herausforderungen stellen Frontend-Entwicklungen wie „Low code/No code", durch bspw. „Drag-and-drop" Tools dar, welche voraussichtlich mehr als 80% der Softwareentwicklung ausserhalb von IT-Abteilungen ausmachen werden[6]. „Chatbots und AI" zur Erstellung von Code durch (intelligente) Code-Vorschläge für Datenanalyse und Testing, „Microservice-Architekturen" mit separierten Code-Basen und Skalierbarkeit sowie Modularität zu erhöhen oder auch die Verwendung von „Voice-Activated-Technologie" für die Steuerung von Smart Homes, Mobiltelefonen und Autosystemen werden Einzug in den operativen Geschäfts- und IT-Alltag halten.

Regulatorische Anforderungen nehmen weiterhin horizontal (mehr beaufsichtigte Unternehmen) und vertikal (detailliertere Vorgaben) zu

Regulatorische Herausforderungen entstehen für Unternehmen in allen Industrien. Vor allem betroffen sind Unternehmen, die in kritischen Infrastrukturbereichen als Anbieter agieren. Durch Neueinführung und Weiterentwicklung bestehender Regularien besteht ein hohes Niveau an Vorgaben, die es einzuhalten gilt.

- Einerseits betreffen diese die Finanz-Regulation, welche national von den Bankenaufsichten und Zentralbanken vorgegeben und hinsichtlich dessen Einhaltung überwacht werden. Beispiele hierfür sind Basel III Reformen (Basel IV)[7] und die MaRisk (Mindestanforderungen an das Risikomanagement)[8].

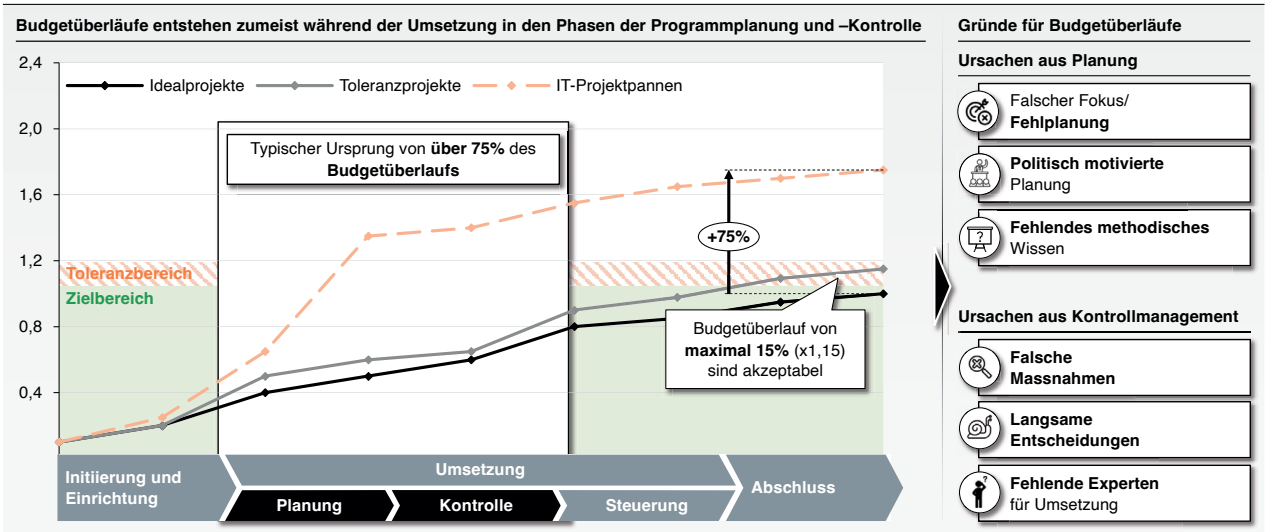
- Andererseits betrifft es die Cybersicherheits-Regulierung, die in Europa durch die NIS2 mit ihrem physischen Pendant der CER sowie dem „Cyber Resilience Act" (CRA)[9], der „Datenschutz-Grundverordnung" (DSGVO)[10] oder auch dem Gesetz zur „digitalen operativen Resilienz im Finanzsektor" (DORA)[11] geregelt, und ausserhalb der EU durch nationale Gesetze gesteuert wird. Weitere Erkenntnisse und Vertiefungen zu den einzelnen Regularien können dem Grey Swan White Paper „Wandel der regulatorischen Welt – NIS2, CER und DORA fordern Wirtschaft heraus" (2024) entnommen werden.

- Die ESG-Regulation gewinnt weiter durch strengere Gesetze und härtere Konsequenzen an Bedeutung. Ein Beispiel stellt die ESG EU Corporate Sustainability Reporting Directive (CSRD)[12] dar, die Unternehmen zur nicht-finanziellen Berichterstattung verpflichtet. Zusätzlich fördern Initiativen wie die United Nations Sustainable Development Goals (SDGs)[13] und Frameworks wie die Global Reporting Initiative (GRI)[14] Massnahmen im ESG-Bereich.

Ein Beispiel für die erhöhten globalen regulatorischen Massnahmen ist die Strafe von 25 Mio. US-Dollar, die im September 2023 von der US-Börsenaufsichtsbehörde SEC gegen die DWS wegen Nichteinhaltung regulatorischer Anforderungen verhängt wurde. Erstens wurde kritisiert, dass die DWS ein unzureichendes Anti-Geldwäsche-Programm für ihre Investmentfonds hatte,

mit mangelnder Umsetzung erforderlicher Richtlinien und unzureichenden Schulungen des Managements. Zweitens wurden falsche Angaben von Seiten der DWS zu ihrem Anlageprozess publiziert, wobei wesentliche Aspekte zwischen 2018 bis 2021 nicht effektiv umgesetzt wurden, was zu irreführenden Informationen über ESG-Praktiken führte[15]. Ebenso wurde der Crédit Agricole im Jahr 2022 von der französischen Finanzaufsichtsbehörde, für Mängel bei der Transaktionsüberwachung und der Sorgfaltspflicht gegenüber Kunden, eine Geldstrafe von 1,5 Mio. € auferlegt[16].

Entwicklung der Budgetkosten von IT-Grossprojekten



Quelle: University of Oxford

Abbildung 3: Entwicklung von Kosten bei IT-Grossprojekten

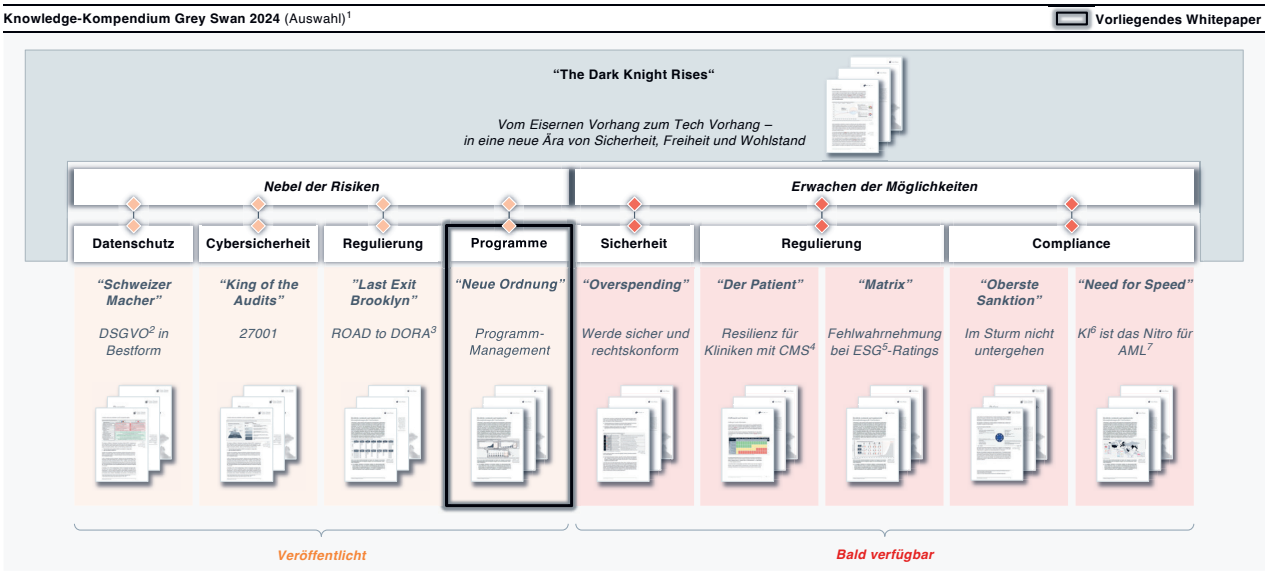
Diese Herausforderungen erfordern ein Management durch zeitlich begrenzte Projekte mit definiertem Umfang und Budget. Dafür sind methodisches Wissen, Tool-Unterstützung und der Zugang zu Experten notwendig. Beispiele hierfür sind IT-Audits (z.B. Solarisbank[17], N26[18]), Digitalisierungsprojekte wie die Modernisierung der IT-Landschaft durch Implementierung neuer Software (z.B. DB-Postbank[19], Deutsche Bahn[20]), Integration von KI-Plattformen (z.B. Vodafone[21], Siemens[22]) und Mergers & Acquisition Transaktionen (z.B. ROHM Co. Ltd Akquisition[23], Microsoft[24]). Diese Vorhaben tragen zu strategischen Unternehmenszielen bei, betreffen übergreifend Unternehmensbereiche und sind durch ihre Komplexität gekennzeichnet.

Effektives Programmmanagement, bestehend aus aufeinander abgestimmten Projekten, ist für den Erfolg solcher Initiativen entscheidend. Wird kein effektives Programmmanagement angewendet, laufen Programme Gefahr in erhebliche Scope-, Time- und Budget-Überschreitungen zu laufen (Abbildung 3).

Im Folgenden erörtern wir Erfahrungen vor dem Hintergrund der Gestaltung und Steuerung hochkomplexer Programme am Beispiel eines IT-Audits. Alle Industrien, die als kritische Infrastruktur eingestuft sind, wie Telekommunikation, Energie, Finanzwesen und auch Gesundheitswesen, müssen IT-Audits durchführen (lassen). Ebenso müssen Finanzunternehmen IT-Audits bestehen, derzeit mit nationalen Regularien unter dem Dach der europäischen Fachaufsichten - European Banking Authority (EBA[25]), European Insurance and Occupational Pensions Authority (EIOPA[26])

und European Securities and Markets Authority (ESMA[27]) als auch der jeweiligen nationalen Aufsicht, ab Anfang 2025 unter der DORA.

Diese Whitepaper trägt zu einem umfassenden Wissenskompendium bei, das unter anderem Fachwissen in den Bereichen Datenschutz, Cybersicherheit und rechtliche Rahmenbedingungen umfasst (Abbildung 4).



Quelle: Grey Swan I 1: Weitere Veröffentlichungen auf Anfrage erhältlich I 2: DSGVO = Datenschutz Grundverordnung I 3: DORA = Digital Operational Resilience Act I 4: CMS = Compliance Management System I 5: ESG = Environmental, Social, Governance I 6: KI = Künstliche Intelligenz I 7: AML = Anti-Money Laundering (Geldwäschebekämpfung)

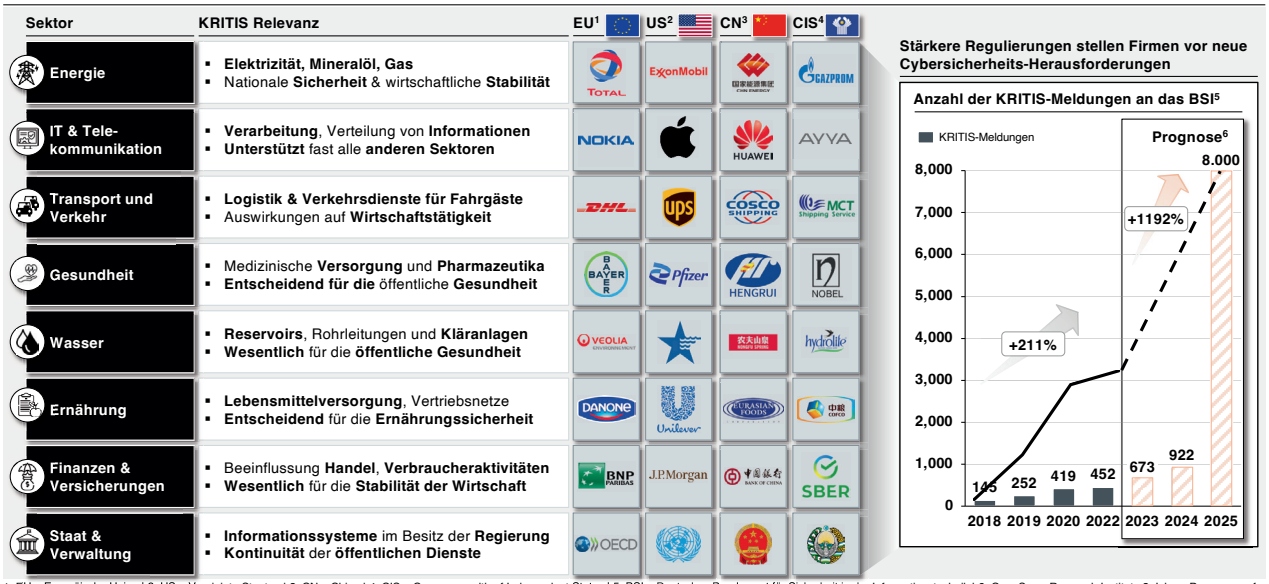
Abbildung 4: Überblick über die Kompetenzbereiche

Wir werden zunächst auf die aufsichtsrechtlichen Entwicklungen im Finanzmarkt mit Blick auf IT-Audits eingehen, gefolgt von der Thematisierung der Herausforderungen in der Verarbeitung der regulatorischen Anforderungen durch das Aufsichtsobjekt. Nachfolgend erläutern wir Lösungsmuster für das Management eines Audits, um abschliessend die Frage zu erörtern, wie eine erfolgreiche Aufstellung im Projektmanagement in der Organisation verankert werden kann.

Aufsichtsrechtliche Entwicklungen steigern regulatorische Herausforderungen

Die Bedeutung kritischer Infrastrukturen (KRITIS) für das staatliche Gemeinwesen und deren Einstufung in verschiedene Branchen wie Energie, IT und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung sowie Staat und Verwaltung ist evident[28]. Diese Branchen sind aufgrund ihrer zentralen Rolle für die Funktionsfähigkeit des Gemeinwesens und der damit verbundenen Risiken im Falle von Ausfällen oder Beeinträchtigungen relevant, daher werden hier aktive KRITIS-Meldungen an den Regulator gefordert (Abbildung 5).

Daten- und Cybersicherheit in 8 kritischen Infrastruktursektoren (KRITIS) ist für Wirtschaftstätigkeit, öffentliche Gesundheit und nationale Sicherheit unerlässlich



1: EU = Europäische Union I 2: US = Vereinigte Staaten I 3: CN = China I 4: CIS = Commonwealth of Independent States I 5: BSI = Deutsches Bundesamt für Sicherheit in der Informationstechnik I 6: Grey Swan Research Institute 3-Jahres Prognose auf Basis von 2 Push Faktoren (Effekte aus Digitalisierung und Erhöhung der betroffenen Unternehmen auf ca. 30.000 durch NIS 2 Inkraftsetzung) sowie 1 Pull Faktor (Effekte aus Umsetzung neuer Gesetze)

Abbildung 5: 8 KRITIS-Sektoren für nationale Wirtschaftsfähigkeit und Sicherheit

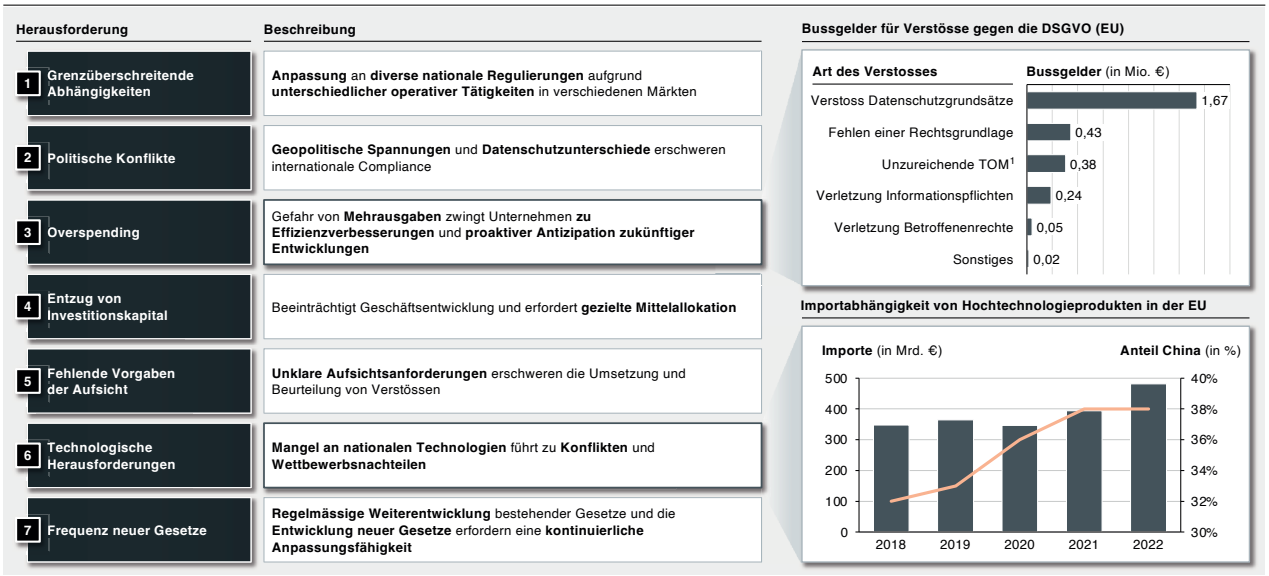
Die durchschnittlichen Kosten für Datenschutzverletzungen betragen 5,04 Mio. USD bei regulatorischen Verstössen in diesen Branchen. Dieser Wert liegt im Durchschnitt um 28,6 % höher als in anderen Sektoren und unterstreicht die Anforderungen an Compliance und Risikomanagement in KRITIS-Unternehmen. Dies führt zu der Frage, wie sich die aufsichtsrechtlichen Rahmenbedingungen für KRITIS-Unternehmen entwickeln und verändern, um deren Funktionsfähigkeit zu sichern.

Bis 2025 werden in Europa und in der Schweiz fast alle relevanten und übergeordneten KRITIS Gesetze aktualisiert oder neu eingeführt. Die Netzwerk-Informationssicherheits-Richtlinie in der Version 2.0 (NIS2)[29] weitet im Vergleich zur NIS1-Version[30] Cybersicherheitsvorgaben auf mehr Sektoren und mehr Unternehmen aus. Für den Finanzsektor kommt die Lex-specialis-Regelung zum Tragen. Sie regelt die Fälle, in denen sowohl DORA als auch die NIS2-Richtlinie Vorgaben machen: Sofern die Anforderungen in DORA spezifischer sind, müssen diese im Vergleich zu den Anforderungen der NIS2-Richtlinie vorrangig beachtet werden. Die finale Regulierung bleibt dem NIS2-Umsetzungsgesetz vorbehalten. In dem Whitepaper “König der Prüfungen”, Grey Swan 2024, wird diese regulatorische Entwicklung im Detail und mit Lösungsmustern erläutert.

7 Hürden für Unternehmen in der Umsetzung von aufsichtsrechtlichen Anforderungen

Das breit gefächerte Thema Compliance steht seit jeher unter dem Generalverdacht einzig Kostenstelle zu sein. Ähnlich wie bei Sicherheit und Datenschutz sollen Arbeiten an den als oktroyiert wahrgenommen Aufgabenstellungen innerhalb der Compliance den Betriebsablauf nicht stören. Nach Möglichkeit sollen interne wie externe Aufwände gering sein. Solange nichts „passiert“ ist alles „gut“.

Herausforderungen in der Verarbeitung der regulatorischen Anforderungen durch das Aufsichtsobjekt



Quelle: Grey Swan I 1: TOM = technisch-organisatorische Massnahmen

Abbildung 6: Herausforderungen durch regulatorische Anforderungen sind vielfältig

Allenfalls akzeptiert wird der Wertbeitrag in Form von verhinderten Sanktionen wie Bussgeldern, Wachstumsbeschränkungen bei Neukunden pro Zeitraum oder die Beschränkung der maximal auskehrbaren Kreditsumme oder gar direkte Massnahmen gegen das Führungspersonal. Die Ergebnisse dieser Herangehensweise zeigen sich in nicht-monetären, monetären und legalen Folgen.

Compliance ist daher kein zeitgeistiges Thema wie ChatGPT bzw. KI. Denn Compliance bietet weit mehr als „nur“ die Einhaltung von gesetzlichen und selbst auferlegten Regelungen. Der Grundkonflikt zwischen „Produktion durch IT“ und „Compliance der IT“ wird trotz vollständiger Digitalisierung das beherrschende Thema der nächsten Jahre. Ab Januar 2025 ist die DORA vollständig anzuwenden.

Flankiert durch weitere europäische und nationale Sicherheitsregelungen, wie beispielsweise NIS2 und CER, ist von einer Anforderungsdynamik vergleichbar bei der Einführung der DSGVO auszugehen. Weiterhin werden sich innerbetriebliche Konflikte durch ein fachlich unterschiedliches Verständnis in der Durchsetzung von Risikosteuerung, in der Arbeitskultur, aber auch durch die unterschiedliche Bewertung von Steuerungsmöglichkeiten operationeller Risiken durch in sich resiliente Systemarchitekturen ausweiten. Herausforderungen in der Verarbeitung der regulatorischen Anforderungen durch das Aufsichtsobjekt können daher unterschiedlich gelagert sein (Abbildung 6).

1. Die meisten KRITIS-Unternehmen sind gleichzeitig in unterschiedlichen Märkten operativ tätig und damit mehreren nationalen regulatorischen Realitäten ausgesetzt (Cross-Market Abhängigkeit). Die erhöhte Komplexität stellt eine massive Herausforderung für die Compliance Abteilungen und das Management dar.

2. Das geopolitische Umfeld zeigt politische Unwägbarkeiten als relevante Barrieren in der Umsetzung von regulatorischen Anforderungen. Einerseits ist De-Risking gefordert. Die Beschaffung von Rohstoffen, der Einsatz von Technologien und der Umgang mit Wissen werden strenger reglementiert. Gleichzeitig stehen sich Europa, die USA und China mit konträren Ansätzen beim Datenschutz gegenüber. Schon immer unterliegt der Wissenstransfer politischen Interessen. In der Summe sind diese Unwägbarkeiten bei der Umsetzung von Projekten mit internationalen Partnern oder Dienstleistern ebenfalls zu berücksichtigen.

3. Das Finanz-Management steht häufig vor dem Problem des „Overspending" für Compliance-Anforderungen, da eine Nicht-Einhaltung einer gesetzlichen Anforderung mit empfindlichen Sanktionen und die nachträgliche Korrektur mit hohen Zusatzkosten verbunden ist. Es steht somit vor der Herausforderung, die Effizienz zur Einhaltung von aufsichtsrechtlichen Entwicklungen zu verbessern und zukünftige Entwicklungen aufwandsarm zu antizipieren. Eine Lösung, um Overspending im Bereich Compliance und Informationssicherheit zu vermeiden, wird in dem Whitepaper „Overspending", Grey Swan 2024, erläutert.

Komplexere Regulationsanforderungen lassen die Bedeutung von Projekt- und Programmmanagement steigen

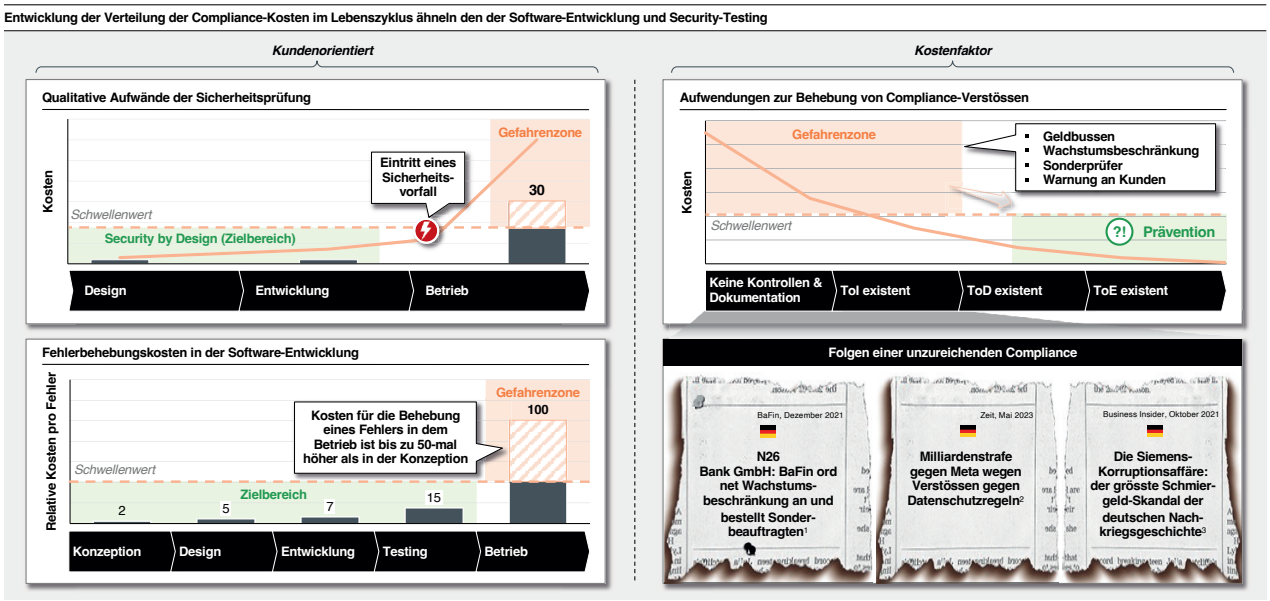
4. Einhergehend mit dem Overspending ist der Entzug von Investitionskapital, sodass zukünftige Investitionen im Geschäftsaufbau geringer ausfallen als bei einer zielgenauen Allokation der verfügbaren Mittel.

5. Eine weitere Herausforderung sind die fehlenden Vorgaben seitens der Aufsicht. Weder die Umsetzung von Anforderungen als auch die Auslegung der Schweregrade einer potenziellen Feststellung sind festgelegt. Die Organisationen empfinden sich mit Blick auf das Lieferkettensorgfaltspflichtengesetz (LkSG) zu 63 % eher mittelmässig bis sehr schlecht vorbereitet31.

6. Die Umsetzung bedeutet für betroffene Unternehmen aufgrund der technologischen Realitäten ihrer installierten Basis eine Herausforderung. Aufgrund der Nichtverfügbarkeit nationaler Infrastruktur-Technologien, deren Einsatz für die Durchsetzung von Effizienzvorteilen zwingend notwendig ist, muss auf internationale Technologien zugegriffen werden, welches zu Konflikten mit dem Regulator oder gar zu Wettbewerbsnachteilen führt. Internationale Technologieanbieter setzen nur widerwillig und zurückhaltend Anforderungen nationaler Regulatoren um. Auch die Sicherstellung einer cyberresilienten Lieferkette, in der Unternehmen ihre eigenen Lieferketten überprüfen müssen aber auch die ihrer Zulieferer stellt sich problematisch dar.

7. Die Frequenz der Veröffentlichung von Gesetzen sowie die Aktualisierung und Veränderung der Anforderungen in bestehenden Werken erfordert einen kontinuierlichen Prüfungsprozess, ob und welche aufsichtsrechtlichen Anforderungen in Anwendung sind oder kurzfristig bevorstehen, sodass diese prozessual, organisatorisch und technisch implementiert werden können. Beispielsweise wurde in NIS2 die Bemessungsgrundlage für KRITIS-Unternehmen daraufhin verändert, dass nicht mehr die Erzeugnisse, wie die aufbereitete Menge Trinkwasser pro Jahr, als Bemessungsgrundlage dient, sondern eine festgelegte Einstufung: Elf Sektoren werden mit hoher und sieben mit sonstiger Kritikalität eingestuft. Welche Einrichtungen als wesentlich („essential“) und welche als wichtig („important“) eingestuft werden, bestimmt sich somit aus der Zugehörigkeit zu einem bestimmten Sektor und der Grösse, gemessen an Umsatz und der Zahl der Mitarbeitenden.

Abbildung 7 zeigt Zusammenhänge aus der Nichtberücksichtigung der vorstehenden sieben Punkte auf. Es wird deutlich, dass die Unternehmen in KRITIS-Sektoren, aber auch in benachbarten Sektoren, aufsichtsrechtliche Entwicklungen beobachten, regelmässig deren Einhaltung prüfen und die Umsetzung sicherzustellen haben.



Quelle: Grey Swan I 1: BaFin I 2: Zeit I 3: Business Insider

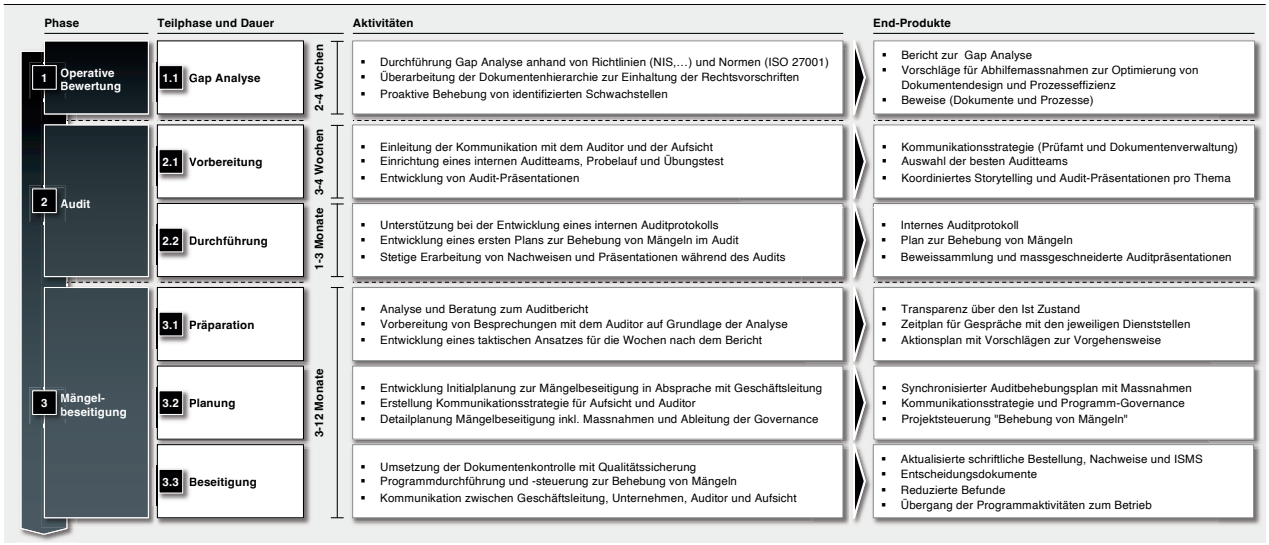
Abbildung 7: Gleichverteilung der Fehlerbehebungskosten im Lebenszyklus essenzieller Prozesse

Das Grey Swan Audit Framework zur Überwindung der Hürden

Für Auditsituationen im Bereich der kritischen Infrastrukturen ist es erfolgskritisch, einen verbindlichen Rahmen für den gesamten Prozess ab Ankündigung des Audits bis zur Mängelbeseitigung vorzugeben.

Es bietet sich an, ein Framework zu nutzen, welches als Orientierungshilfe dient und eine konsequente Unterscheidung nach Auditphasen mit phasenübergreifenden Aktivitäten verbindet. Je nach Phase stehen unterschiedliche Aktivitäten und Ergebnisobjekte im Fokus, die durch eine passgenaue Herangehensweise sichergestellt werden. Wenngleich die Anwendung eines Frameworks, insbesondere bei komplexeren Auditsituationen, in denen die Auditvorbereitung und -durchführung den Aufbau einer standhaften sowie professionellen Verteidigungslinie benötigen und die Mängelbeseitigung nur in Form eines Programms zu bewältigen ist, eine kritische Rolle einnimmt, ist die Anwendung eines Frameworks grundsätzlich ratsam.

Das Grey Swan Audit Framework umfasst 3 Phasen mit insgesamt 6 Unterphasen und entsprechenden End-Produkte



Quelle: Grey Swan

Abbildung 8: Das Grey Swan Audit Framework

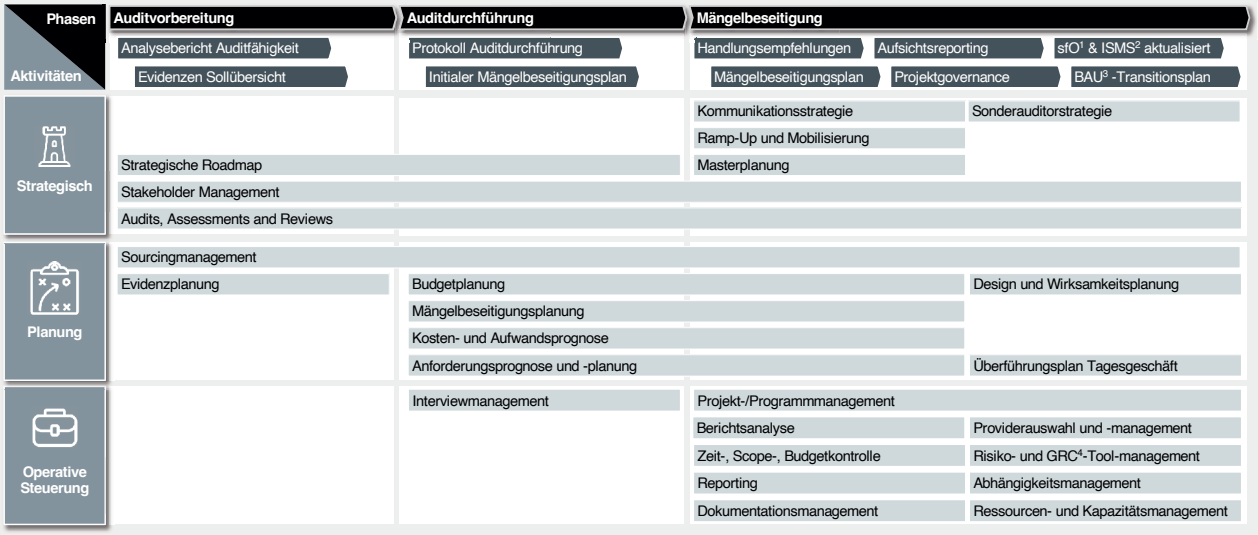
So können bestmögliche Ergebnisse im Audit und für den Auditbericht erzielt werden, um bereits vor der Mängelbeseitigung den grösstmöglichen Einfluss auf die regelmässige hohen Aufwände nehmen zu können. Das Grey Swan Auditframework fasst vielseitige Erfahrungen aus KRITIS-, Compliance-, ISMS- sowie Programmanagement in einem übergreifenden und erprobten Framework zusammen (Abbildung 8). Das Framework integriert für Auditsituationen konzipierte Methoden und Werkzeuge, die aufeinander abgestimmt sind. So kann eine strukturierte Verfahrensweise durchgesetzt und die Ganzheitlichkeit des Auditmanagements gewährleistet werden. So wird ermöglicht, neuralgische Punkte (beispielsweise der Deltabericht aus der Gap Analyse, Interviews in der Audit-Vorbereitung und -durchführung, die Zusammenarbeit mit den Auditoren, Berichte an die nationale Aufsicht oder der Plan für die Mängelabarbeitung) zu steuern.

Eine Vertiefung des Auditframeworks anhand von Praxisbeispielen und der Anwendung in der Praxis werden durch unsere Grey Swan Compliance Experten im dedizierten Blogpost „Dichtung und Wahrheit“, Grey Swan 2024, thematisiert.

Effektives Programmmanagement ist erfolgskritisch für die Mängelbeseitigung

Die erfolgreiche Durchführung von Projekten und Programmen, dazu sind auch Mängelbeseitigungsprogramme zu zählen, kann durch drei Erfolgsfaktoren sichergestellt werden: methodisches Wissen, Tool-Unterstützung und erfahrene Experten.

Phasen und Aktivitäten im Audit Management



Quelle: Grey Swan I 1: sfO = schriftlich fixierte Ordnung I 2: ISMS = Informationssicherheitsmanagementsystem I 3: BAU = Business-as-Usual I 4: GRC = Governance, Risk and Compliance

Abbildung 9: Phasen und Aktivitäten im Audit und Programm Management

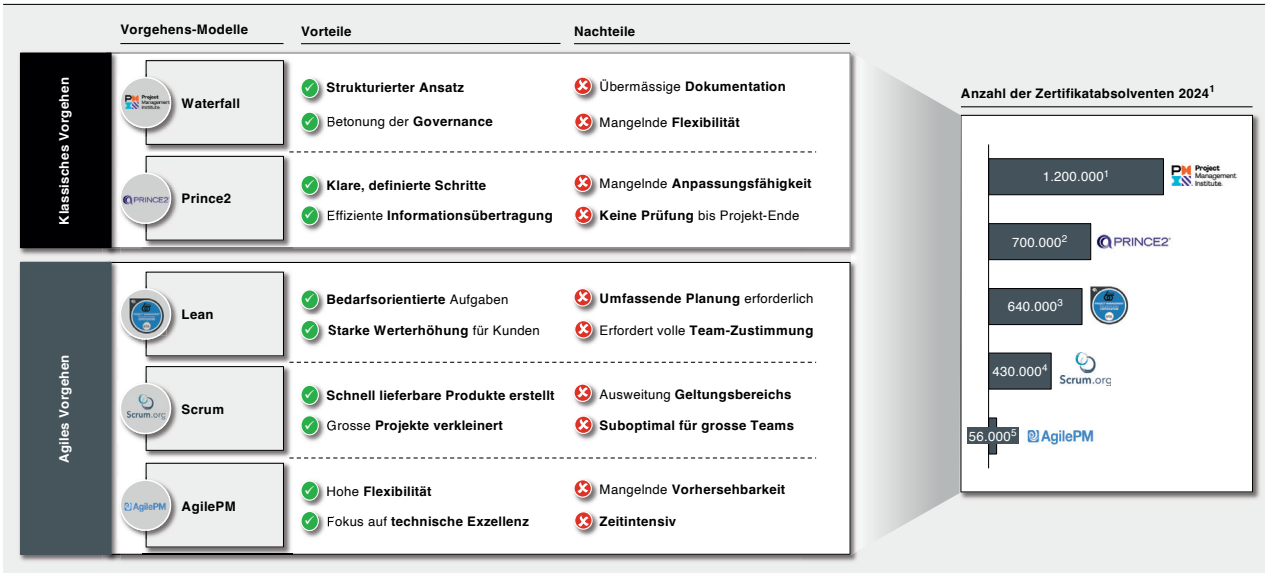
Wenn der Gedanke des Prüfungsframeworks fortgeführt wird und durch ein effektives Programmmanagement gelöst werden soll, ist die Schlussfolgerung ein „Programm Audit Framework“, welches die Phasen der Prüfung mit den Disziplinen des Programmmanagements zusammenführt (Abbildung 9). Es verbindet die Phasen der „operativen Bewertung“, „Audit“ (inkl. Vorbereitung sowie Durchführungsunterstützung) und der „Mängelbeseitigung“ auf der Zeitachse mit strategischen, operativen, Planungs- und Steuerungsaktivitäten auf der Aktivitätenachse mit den jeweils relevanten Inhalten. Beide Achsen zusammen konstituieren eine Matrix, die die Steuerbarkeit von komplexen Projekten in den drei Phasen durch videnzbasierte Scope-Definitionen sicherstellt.

Methodisches Wissen

Eine erste wichtige und notwendige Erkenntnis zur Methodik im Projektmanagement ist die Unterscheidung zwischen Projekten und Programmen, welche sich anhand von der Art des zu erreichenden Ziels (operativ vs. strategisch), Dauer und Zeitrahmen (2-3 Monate vs. 1-3 Jahre), Budget- und Ressourcenbeschränkung (fixes Gesamtbudget vs. periodisches Budget) oder der Kritikalität für das Unternehmen (begrenzt vs. unternehmenskritisch) ermitteln lässt.

Nach dieser Entscheidung muss der passende methodische Ansatz gewählt und als erstes geklärt werden, ob es ein Vorhaben mit grosser Anzahl an Software-Entwicklungsaktivitäten ist. Ist dies der Fall, sollten agile Methodiken wie Lean, AgilePM und Scrum.org Verwendung finden. Handelt es sich um eine andere Art von Vorhaben ohne erhebliche IT-Aufwände, kann ein klassisches Vorgehen nach Waterfall oder Prince2 passender sein (Abbildung 10).

Projektmanagement Vorgehensweisen im Vergleich



Quelle: CRM I 1: Project Management Institute I 2: Prince2 I 3: International Project Management Association I 4: Scrum.org I 5: AgilePM

Abbildung 10: Projektmanager häufiger zertifiziert in klassischen Vorgehensmodellen

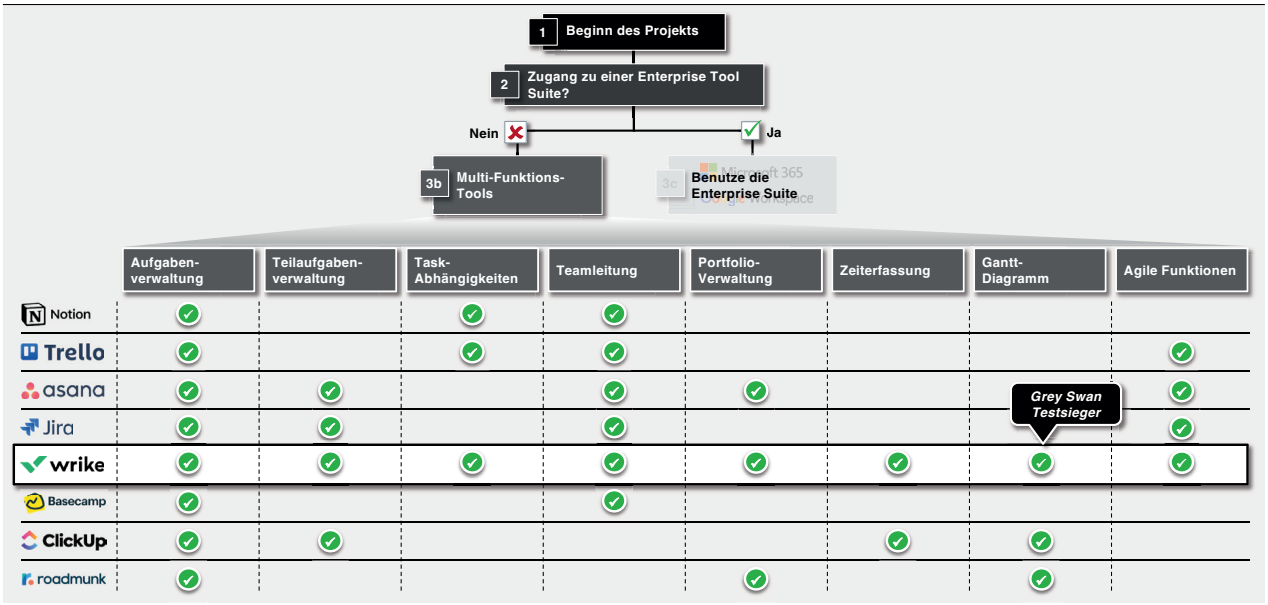
Grundsätzlich sollten Programme einem Lebenszyklus folgen, der die Phasen Initiierung und Setup, Durchführung (inklusive Planung, Kontrolle und Steuerung) sowie Abschluss beinhaltet. Zudem ist bei grösseren Programmen ein hybrider Ansatz häufig passender, d.h. einige Projekte arbeiten agil, andere klassisch nach Wasserfall und auf der obersten Programmebene wird z.B. klassisch geplant und berichtet.

Methodische Kenntnisse sind darüber hinaus auch für die den Phasen zugrunde liegenden Disziplinen erforderlich. Anhand des Vorgehensbeispiels für Programme beinhaltet die Initiierung die Definition der Programmziele, das Aufsetzen der Gremienstruktur oder die Festlegung der Rollen und Aufgaben. Zur Durchführung zählt zum einen die Beherrschung von Ergebnis-, Ressourcen-, Kosten-, Abhängigkeits- und Programmplanung, zum anderen die Kontrolle mit Reporting, Risiko-, Ergebnis- und Abhängigkeitscontrolling und die Programmsteuerung, Massnahmenableitung und das Eskalationsmanagement. Zum Abschluss werden Folgeaktivitäten festgelegt, der Abschlussbericht erstellt sowie das Projekt übergeben.

Tool-Unterstützung

Die richtige Toolauswahl ist entscheidend, um gerade bei komplexeren Projekten spätere unnötige Aufwände für administrative Tätigkeiten zu vermeiden. Ein Bericht des Dimensional Research Instituts zeigt auf, dass die meisten Sicherheitsexperten die Verbesserung der Sicherheitslage ihres Unternehmens durch die Aufrüstung ihrer Tools (67%) als Hauptmethode ansehen. Allerdings werden diese Bemühungen oft durch Probleme bei der Integration, fehlende Expertise und die hohe Anzahl an zu verwaltenden Tools behindert[32]. Daher muss bei der Auswahl der passenden Projektmanagement Tools berücksichtigt werden, welche Softwareanwendungen in der Organisation bereits im Einsatz sind, was mit der Frage nach dem Zugang und der Verfügbarkeit einer Enterprise Tool Suite beantwortet werden kann (Abbildung 11).

Entscheidungsbaum für Projektmanagement Tools



Quelle: Grey Swan Research Institute

Abbildung 11: Wrike Testsieger bei Multifunktionstools

Wird beispielsweise mit einer Enterprise Suite (z.B. Microsoft 365, Google Workspace oder LibreOffice) gearbeitet, sollten die darin integrierten Tools (z.B. MS Teams und MS Project, G Slides und G Meet oder LibreWriter und LibreImpress) genutzt werden. Bei Bedarf können diese um weitere schon in der Suite integrierte Tools (z.B. Confluence) ergänzt werden, da die Mitarbeitenden mit diesen bereits vertraut sind. Sollte kein Zugang zu einer Enterprise Tool Suite bestehen, besteht die Auswahlmöglichkeit einer Single-Use-Lösung, spezialisiert auf eine bestimmte Anforderung, wie beispielsweise Trello für die Aufgabenverwaltung, oder einer Multi-Use-Lösung, die mehrere Anforderungen abdeckt, wie beispielsweise Wrike (unser Testsieger).

Anhand des Beispiels des Reportings vom Anfang lässt sich der Vorteil des richtigen Tools aufzeigen, denn nur mit einem einheitlichen, transparenten und faktenbasierten Reporting besteht die Möglichkeit zur Erstellung von Standardreports für regelmässig tagende Projektgremien, aber auch zur Bedienung von ad-hoc Anfragen und Erhöhung der Effizienz in der Projektsteuerung. Dazu ist für das Reporting ein dediziertes Tool als verpflichtendes und alleiniges Werkzeug für Tracking und Reporting („Single/Golden Source“) der ausgewählten KPIs festzulegen.

Experten

Experten oder Fachexperten (SMEs) sind entscheidend für den Erfolg von Projekten und verfügen über ein umfassendes Wissen in einem speziellen Fachgebiet.

In einer Ära, in der der Zugang zum grenzenlosen Wissen des Internets besteht, mag es so erscheinen, als ob die Welt mit Alleskönnern gespickt ist und Experten durch Nicht-Experten ersetzt werden können, die sich durch Eigenrecherche und ad-hoc Zertifizierungen behelfen. Dies ist jedoch nicht der Fall, insbesondere bei komplexen Transformationsprogrammen mit ehrgeizigen Zeitplänen oder einer Vielzahl von beteiligten Abteilungen und Teams, wo Kompetenz und Erfahrung von entscheidender Bedeutung sind. Die Fähigkeiten von Experten werden über Jahre hinweg entwickelt, sowohl durch praktische Erfahrungen als auch durch kontinuierliche fachliche Ausbildungen und Schulungen in ihrem Bereich.

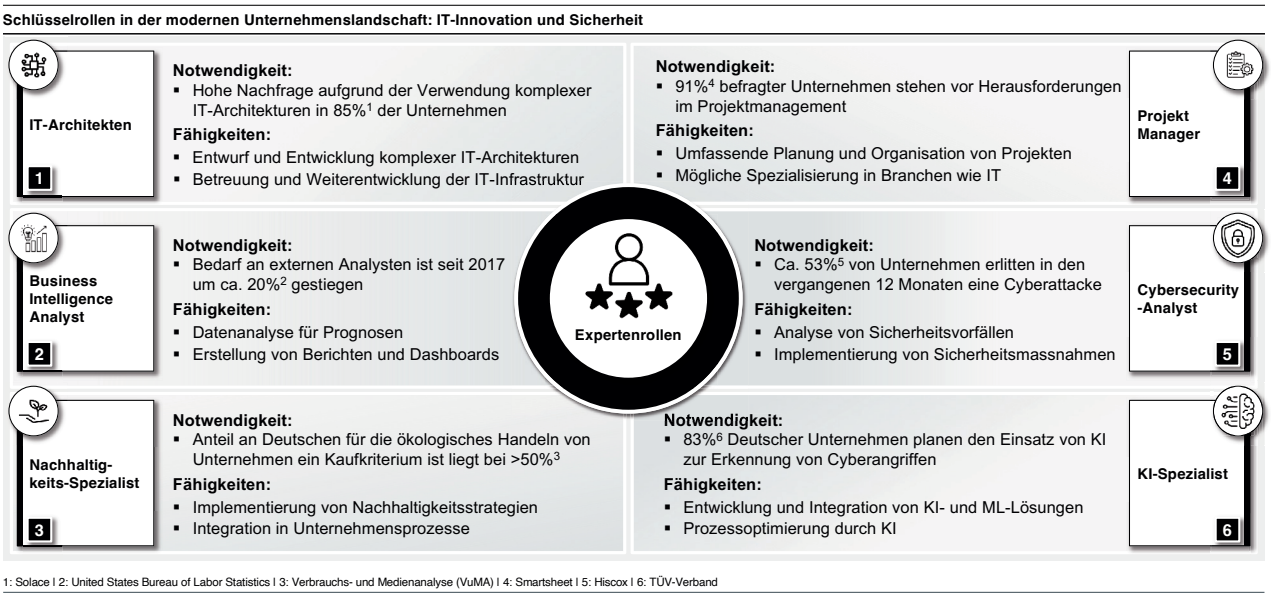


Abbildung 12: Nachfragestarke Experten Positionen

Zur Adressierung der identifizierten Herausforderungen werden insbesondere sechs Experten benötigt (Abbildung 12), um in der modernen Unternehmenslandschaft technologische Innovation, (IT-)Sicherheit und die Verarbeitung von regulatorischen Vorgaben sicherzustellen. Zum Beispiel stehen 91% der befragten Unternehmen vor Herausforderungen im Projektmanagement (Projekt Manager), 85% sehen Experten-Bedarfe zur Verwendung von komplexen IT-Architekturen (IT-Architekten) als notwendig und 83% planen den Einsatz von KI zur Erkennung von Cyberangriffen (KI-Spezialist). Weitere Bedarfe liegen bei den Informationssicherheits- und Cybersecurity-Analysten sowie bei Nachhaltigkeits-Spezialisten.

Lösungsmuster für die Umsetzung eines Mängelbeseitigungsprogramms

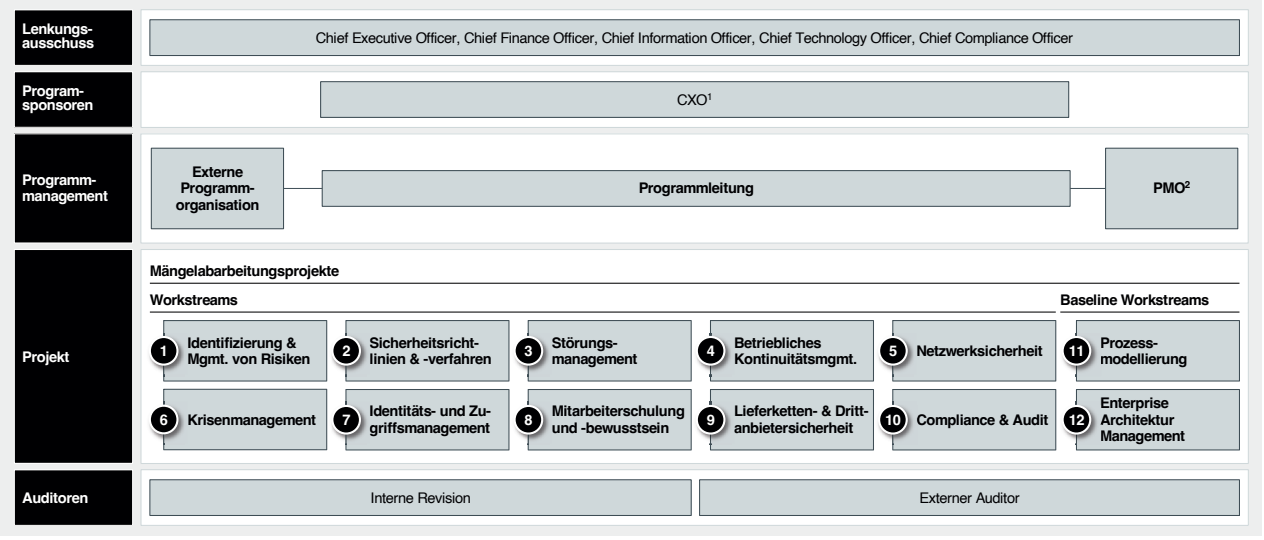
Entscheidende Erfolgsfaktoren für eine zeitgerechte und effektive Umsetzung der Mängelbeseitigung sind:

- Angemessene Governance
- Sachgerechte Kommunikation
- Detaillierter Mängelbeseitigungsplan
- Strukturierter Abnahmeprozess
- Kontinuierliche, faktenbasierte Berichterstattung
- Überprüfung der Massnahmen nach ToD, ToI und ToE
- Nahtlos ineinandergreifender Ende-zu-Ende Ergebnis- und Lieferprozess

Governance

Um eine effektive Mängelabarbeitung zu gewährleisten, ist es zunächst wichtig, eine passgenaue Programmstruktur und Steuerung festzulegen. Hierbei sollten klare Strukturen mit den relevanten Stakeholdern festgelegt werden und einem Lenkungsausschuss, Sponsoren sowie einem zu Entscheidungen ermächtigten Programmmanagement mit Programmleitung plus PMO und den jeweiligen Abarbeitungsprojekten bestehen.

Programmstruktur zur Beseitigung der Mängel in einer komplexen Prüfungssituation



Quelle: Grey Swan I 1: CXO = Verantwortliche C-Levels I 2: PMO = Projekt Management Office

Abbildung 13: Beispielhafte Programmstruktur und Governance

Dabei sollten externe Schnittstellen, wie beispielsweise zum Auditor oder Sonderbeauftragten und der Aufsicht, berücksichtigt werden. Besonders wichtig ist die vollständige Beteiligung der verantwortlichen Mitglieder des Vorstandes im Lenkungsausschuss, um eine optimale Steuerung und Überwachung des Programms sicherzustellen. Die Programmleitung übernimmt die Koordination der Abarbeitungsprojekte und fungiert als Schnittstelle zwischen Führungskräften

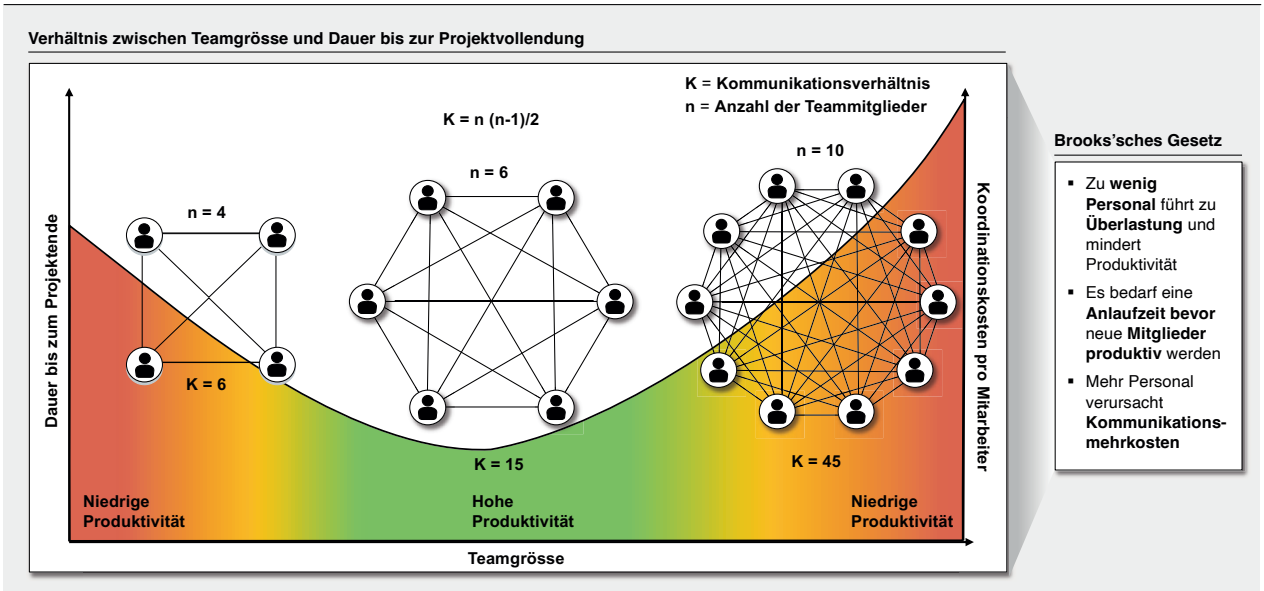
und Sonderbeauftragten. Zur Umsetzung dieser Aufgaben können sowohl ein internes als auch ein externes Projekt Management Office genutzt werden. Um die Programmstruktur effizient aufzustellen, sind die Abarbeitungsprojekte entsprechend der Themengruppen des Mängelbeseitigungsplans zu strukturieren, sodass alle Mängel systematisch erfasst, priorisiert und bearbeitet werden können (Abbildung 13).

Kommunikation mit der Aufsicht und Entwicklung einer Strategie

Zu Beginn der Umsetzung eines Mängelbeseitigungsprogramms liegt der Fokus auf der Kommunikation mit der Aufsicht, mit internen Gremien (Risikomanagement-, Compliance- und Entscheidungsgremium) und Abteilungen.

Zusätzlich muss die Identifikation von Handlungsoptionen erfolgen, sowie die Abwägung und Vorbereitung der Optionen zur Entscheidung. Massstab ist jeweils die Analyse des Prüfberichts. Weiterhin gilt es, die Gesprächsvorbereitung von anstehenden Terminen mit der Aufsicht, basierend auf den Analyseergebnissen, sicherzustellen, sowie die Ausarbeitung eines taktischen und strategischen Vorgehens flankierend mit einer Kommunikationsstrategie vorzunehmen. Programme sind typischerweise unternehmensübergreifend und involvieren diverse Organisationsgruppen, Gremien als auch Abteilungen.

Mit wachsender Anzahl an Teammitgliedern innerhalb eines Projekts steigt die Komplexität der Kommunikation



Quelle: Brooks Jr., F. P.

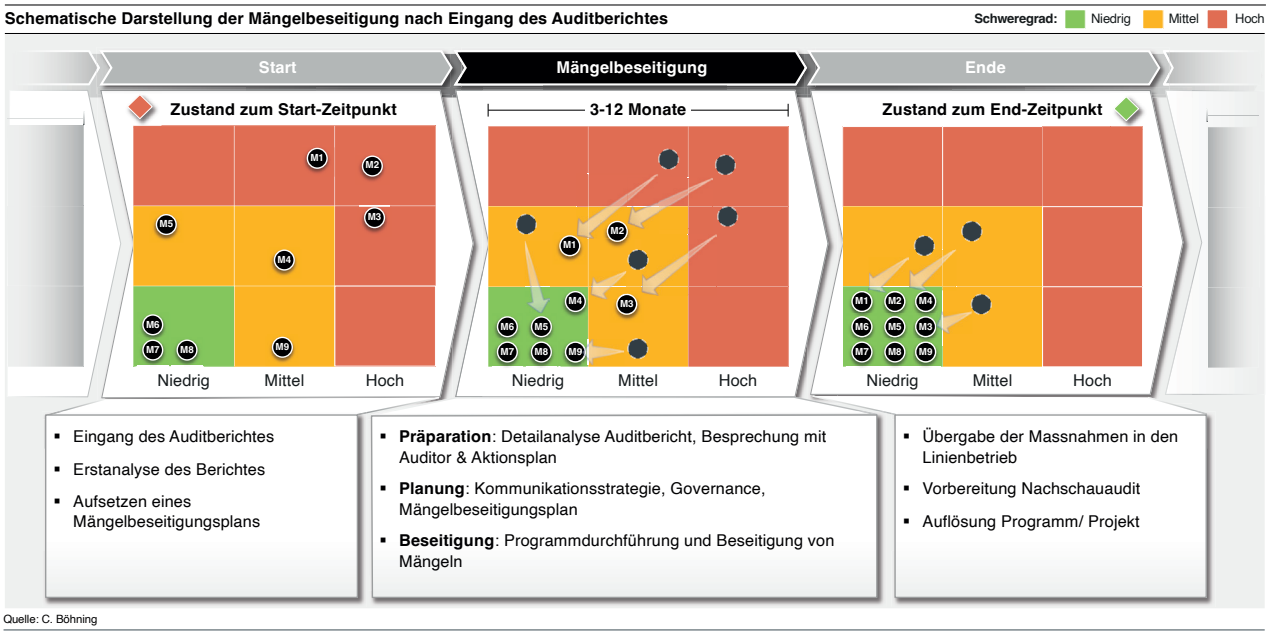
Abbildung 14: Darstellung Brooks'sches Gesetz

Bei der Entwicklung der Kommunikationsstrategie, ähnlich wie bei der Festlegung der Programm-Governance, sollte die bei einem Mängelbeseitigungsprogramm inhärente hohe Anzahl von internen und externen Stakeholdern berücksichtigt werden. Daraus resultiert, dass Auditoren (interne Revision, externer Auditor) in verschiedenen Projekten zur Abarbeitung der Mängel mit Mitarbeitenden aus den dafür verantwortlichen Abteilungen involviert sind.

Zudem werden Projektorganisations-Gremien als auch Entscheider involviert. Daher ist zu vermeiden, dass die Kommunikationsbeziehungen zu einem lähmenden Faktor (Abbildung 14) für den Sachfortschritt werden.

Mängelbeseitigungsplan

Die Aufstellung des Mängelbeseitigungsplan zielt darauf ab, die sfO zu aktualisieren, sodass darin enthaltene Dokumente rechtliche Konformität erhalten, Managemententscheidungen und -freigaben revisionssicher festzuhalten und Feststellungen schlussendlich zu reduzieren und die Programm-Tätigkeiten des Audits in das Tagesgeschäft zu überführen. Hierfür ist die Erstellung eines Mängelbeseitigungsplans, bei dem die Reduzierung der Mängel fokussiert wird, unabdingbar. Zum Beispiel nach dem Vorbild des von C. Böhning, damals tätig bei einem Berliner Technologie-Think-Tank, im Rahmen eines Mängelbeseitigungsprogramms bei einer deutschen international tätigen Grossbank entwickelten Framework (Abbildung 15).



Quelle: C. Böhning

Abbildung 15: Priorisierung der Abarbeitung von Feststellungen

Bevor mit der Reduktion der Feststellungen begonnen werden kann, ist es wichtig, alle Feststellungen nach Schwere (Mängelliste mit Umsetzungsplan nach BaFin), Dringlichkeit und Umsetzbarkeit zu klassifizieren. Eine sorgfältige Bewertung der Feststellungen ist essenziell, um sicherzustellen, dass die begrenzten Ressourcen effektiv eingesetzt werden und eine schnelle Reduktion der Feststellungen erreicht werden kann.

Nachdem eine Bewertung der Feststellungen durchgeführt wurde, ist eine schnelle Reduktion der „hoch/sehr hoch“ resp. F3/F4-Feststellungen zu fokussieren, damit ein stabiler Zustand erreicht wird. Hierbei sollten die erfolgskritischsten Abarbeitungsprojekte priorisiert und aufeinander abgestimmt werden. Während der Beseitigung liegt der Fokus auf der Ergebnissicherung der bereits abgearbeiteten „hoch/sehr hoch“-Feststellungen. Zusätzlich dazu wird die Abarbeitung

der nicht erfolgskritischen Feststellungen („niedrig“ und „mittel“ resp. F1/F2) fokussiert, um eine solide Basis für den Normalbetrieb zu schaffen. Die implementierten technisch-organisatorischen Massnahmen werden auf ihre Wirksamkeit überprüft und gegebenenfalls angepasst.

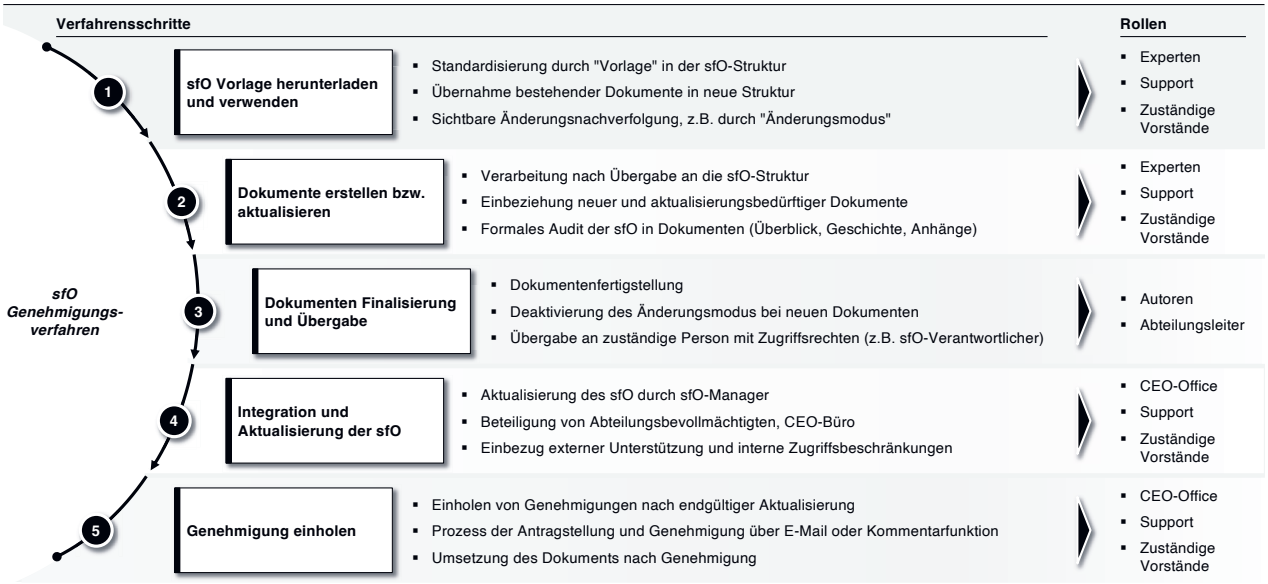
Sobald eine ausreichende Wirksamkeit (ToE) in Form der beschriebenen (ToD) und implementierten (ToI) Prozesse nachgewiesen wurde und die nicht erfolgskritischen Feststellungen abgearbeitet wurden, sind Review und Abschluss des Mängelbeseitigungsplans einzuleiten.

Ziel dabei ist, die verbliebenen Feststellungen der Schwere „niedrig“ und „mittel“ in den Normalbetrieb zu überführen und alle Feststellungen abzumelden. Nach der erfolgreichen Abmeldung der Mängelbeseitigung durch das Aufsichtsobjekt und der Freigabe durch den Auditor bzw. die Aufsicht ist eine langfristige operationelle Stabilität zur Erhaltung der IKT-Reife der Organisation sicherzustellen; diese umfasst ebenso die Vorbereitung auf einen eventuellen Nachschauaudit.

Abnahmeprozess

Die Erstellung und Aktualisierung sämtlicher Dokumente sind systematisch und kontrollierbar durchzuführen, um sicherzustellen, dass die Nachvollziehbarkeit und Transparenz von Änderungen gegeben ist. Es bietet sich an, einen geeigneten Abnahmeprozess zu definieren, bei dem Anforderungen und die Verantwortlichkeiten festgelegt werden (Abbildung 16).

Die Aktualisierung der schriftlich fixierten Ordnung erfolgt eines vorgegebenem Genehmigungsverfahren: Schritte und Rollen



Quelle: Grey Swan

Abbildung 16: Exemplarisches Genehmigungsverfahren für Dokumente der sfO

Zunächst sollte eine Vorlage für die sfO festgelegt sein, die alle notwendigen Informationen und Anforderungen an alle Dokumente enthält (z.B. Dokumenteninformationen, Versionierungshistorie, einheitliches Inhaltsverzeichnis) und als Grundlage für die Aktualisierung sowie die Erstellung neuer Dokumente dienen kann. Auf Basis dieser können die jeweiligen Abteilungen oder Experten Dokumente erstellen und bestehende Dokumente in die Vorlage (das Template) überführen.

Nach anschliessender Aktualisierung und Erstellung der Dokumente sollte vor der Finalisierung durch die Autoren und Experten geprüft werden, ob die formalen Aspekte der sfO im Dokument reflektiert sind, bevor diese an die Verantwortlichen der sfO übergeben werden.

Die sfO-Verantwortlichen (z.B. bevollmächtigte Personen der Abteilung, das CEO-Office oder externe Unterstützung) integrieren die Änderungen und beginnen mit der Einholung von Genehmigungen. Diese Beantragung kann auf unterschiedliche Weise erfolgen, bei der sichergestellt werden sollte, dass sie konsistent, nachvollziehbar und transparent sind, damit diese Dokumente in Kraft treten können. Es bietet sich z.B. an, Kommentarfunktionen bei Confluence zu verwenden oder E-Mail-Nachweise an geeigneter Stelle zu hinterlegen.

Es ist wichtig zu betonen, dass die Aktualisierung der sfO kein einmaliger Prozess ist, sondern regelmässig und anlassbezogen durchgeführt wird. So können mögliche Schwachstellen und Risiken identifiziert werden, um eine angemessene Sicherheit im Unternehmen zu gewährleisten.

Faktenbasierte Berichterstattung

Die Kontrollen der drei Verteidigungslinien (ToX) sind wesentliche Elemente des Berichtswesens

Mit der Einführung eindeutiger Bezeichnungen von Nachweisen sowie der Aktualisierung des Mängelbeseitigungsplans wird fortlaufend eine übergreifende Transparenz geschaffen, welche in Kombination mit einem wiederkehrenden Reporting den Erfolg weiter festigt. Dabei ist der Abarbeitungsstand der einzelnen Nachweise in standardisierter Form zu erfassen. Dies kann als eine Art Frühwarnsystem genutzt werden. Dieses Frühwarnsystem ermöglicht die Entdeckung von Problembereichen und die Einleitung von Massnahmen auf objektiver Basis.

Um die Bewertung des Fortschritts der Nachweise zu vereinfachen und mögliche Fehler zu vermeiden, ist es empfehlenswert, einen standardisierten und auf Feststellungen sowie Unterfeststellungen abgestimmten Reporting-Workflow sowie einen Leitfaden für die Berichterstattung zu entwickeln. Solch ein Workflow beinhaltet unterschiedliche Status mit definierten Beschreibungen sowie einer Definition des Abarbeitungsstands, wodurch eine standardisierte Fortschrittsbewertung über Abarbeitungsprojekte hinweg ermöglicht wird. Wenn alle einer Feststellung zugrunde liegenden Nachweise im Reporting denselben Status haben, erbt die (Unter-)Feststellung diesen Status.

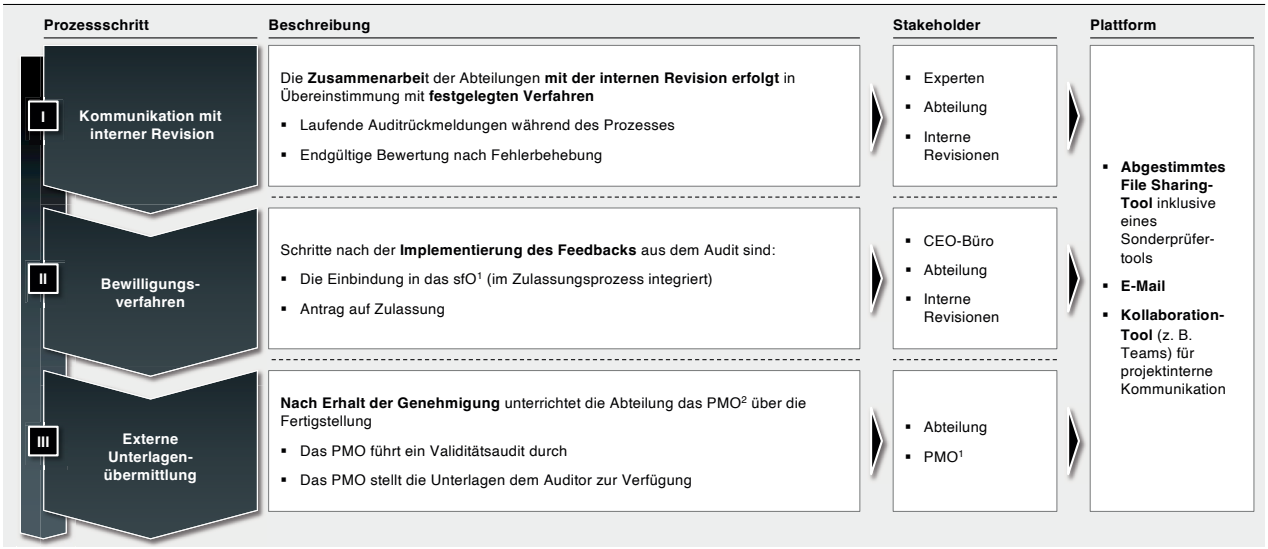
Im Fall eines gemischten Status erbt der Gesamtstatus den niedrigsten Status der Nachweise. Das Reporting kann beliebig von einer monatlichen auf eine zwei- oder sogar eine wöchentliche Basis für das Management oder einem unabhängigen Dritten heruntergebrochen werden und so eine Rückverfolgbarkeit ermöglichen.

Ende-zu-Ende Lieferprozess

Das Bindeglied zur Sicherstellung einer hohen Qualität der Dokumente, der regulatorisch geforderten Ablage und dem faktenbasierten Reporting ist ein Ende-zu-Ende-Lieferprozess. Dieser Prozess steuert die Interaktion mit der internen Revision, dem Auditor oder dem externen Sonderbeauftragten sowie den verantwortlichen Autoren der Dokumente, wodurch frühzeitig Feedback eingeholt und in Abstimmung mit der internen Revision eingearbeitet werden kann (Abbildung 17).

Die Interaktion zwischen den Abteilungen und der internen Revision muss nach Vorgaben erfolgen, da diese eine unabhängige Bewertungsinstanz darstellt und nicht als Quality Gate bei einzelnen Dokumenten fungiert. Aus diesem Grund wird, nachdem alle Mängel behoben wurden, ein formelles Auditurteil von der internen Revision erstellt. Um eine Genehmigung bzw. Feedback für die behobenen Mängel zu erhalten, muss ein vorgegebenes Genehmigungsverfahren durchlaufen werden, bei dem explizit durch das Projektteam eine Anfrage bei der internen Revision samt allen Dokumenten eingeht. Sobald die Genehmigung erteilt wurde, erfolgt die endgültige Finalisierung der Dokumente.

Ein durchgehender Prozess für die Dokumenteneinreichung gewährleistet die Erstellung von qualitativ hochklassigen Unterlagen



Quelle: Grey Swan I 1: sfO = schriftlich fixierte Ordnung I 2: PMO = Project Management Office

Abbildung 17: Prozess zur Dokumenteneinreichung

Das PMO führt ein Plausibilitätsaudit durch und stellt die Dokumente dem Sonderbeauftragten zur Verfügung. Auch hier werden definierte File-Sharing-Tools und E-Mail-Systeme verwendet, um die Dokumente sicher und effizient zu teilen. Dieser Ende-zu-Ende-Lieferprozess ermöglicht es den Abteilungen, Experten, der internen Revision und anderen Stakeholdern, qualitativ hochwertige Dokumente zu erstellen, dass diese ordnungsgemäss genehmigt werden. Kommunikation, Verantwortlichkeiten und Prozesse sind entscheidend, um eine reibungslose Zusammenarbeit und eine effiziente Dokumentenerstellung zu gewährleisten.

Überprüfung der Massnahmen nach Test-of-Design, Test-of-Implementation und Test-of-Effectiveness

Sobald Massnahmen gemäss des Reportings abgemeldet werden, wird im nächsten Schritt eine Überprüfung auf deren Effektivität notwendig sein. Hierbei werden die Massnahmen entsprechend der Umsetzung der Soll-Massnahmen (Test-of-Design) sowie deren tatsächliche Wirksamkeit bewertet (Test-of-Effectiveness). Der Test-of-Design prüft, ob die technisch-organisatorischen, rechtlichen und personellen Massnahmen des Unternehmens den Anforderungen der gesetzlichen Vorgaben entsprechen und in der schriftlich fixierten Ordnung (sfO) als Soll-Vor-

gabe vorliegen. Neben der Erfüllung der Formalien der sfO wird insbesondere untersucht, ob die erforderlichen Kontroll- und Überwachungsmechanismen zur Gewährleistung der Einhaltung der gesetzlichen Anforderungen vorhanden sind. Dazu gehört beispielsweise der Audit, ob Verantwortlichkeiten, Befugnisse und Kompetenzen geregelt sind, ob es ausreichende interne Kontrollen und Auditmechanismen gibt und ob die Einhaltung von internen Richtlinien und Vorgaben durch angemessene Kontrollen überwacht wird.

Der Test-of-Implementation (ToI) prüft aufbauend darauf ob Kontrollen vorhanden sind, welche in die betrieblichen Abläufe integriert und umgesetzt werden. Hierbei wird untersucht, ob die in der sfO definierten Soll-Massnahmen nach gesetzlichen und internen Vorgaben implementiert sind. Mögliche Belege, die für die Überprüfung der Implementierung dienen, sind beispielsweise Veröffentlichungen im organisationsinternen Wiki, die Verteilung/Präsentation bei Besprechungen oder die Bestätigung der Kenntnisnahme im HR-Management-Tool.

Das ToX-Modell (ToD, ToI, ToE) ist essenziell für eine erfolgreiche Projektorganisation für IT-Audits

Beim Test-of-Effectiveness (ToE) wird überprüft, ob die im ToI eingeführten Kontrollen effektiv nach ihrer Definition (ToD) umgesetzt (ToI) wurden und in der Praxis effektiv, d.h. gemäss den gesetzlichen und internen Anforderungen funktionieren. Die Operationalisierung der Kontrollen kann in verschiedenen Dimensionen stattfinden, wie z.B. Schulung des Personals, Bereitstellung von Kommunikationsnachweisen sowie Bestätigung der Wirksamkeit durch interne oder externe Auditoren. Um den ToE durchzuführen, sind Nachweise durch die interne Revision zu prüfen, die eine Umsetzung der Kontrollen belegen. Dabei sollten die Nachweise den Status der Operationalisierung widerspiegeln, um einen Überblick über den Fortschritt zu geben und mögliche Abweichungen zu identifizieren. Es ist wichtig, dass die Operationalisierung der Kontrollen kontinuierlich überwacht und bei Bedarf angepasst wird. Insgesamt trägt der ToE dazu bei, Schwachstellen in der Umsetzung der Kontrollen aufzudecken und gegebenenfalls Korrekturmassnahmen einzuleiten, um das Risiko von Fehlern und Compliance-Verstössen zu minimieren.

Verankerung des Programmmanagements in der Organisation als weiterer Erfolgsfaktor

Unabhängig davon, welche Art von Herausforderung, politisch, technologisch oder regulatorisch gemeistert werden muss, zeigt die Erfahrung, dass die Beherrschung der Projekt- und Programmmanagement Disziplinen in der Organisation ein übergreifender Erfolgsfaktor ist. Für die Beherrschung wurden drei zugrundeliegende Erfolgsfaktoren erörtert: methodisches Wissen, Tool-Unterstützung und erfahrene Experten. Der letzte Punkt ist entscheidend für die Verankerung des Projekt- und Programmmanagements in der Organisation und bietet drei Umsetzungsoptionen: Insourcing, Outsourcing und Hybrid (Abbildung 18).

Im Rahmen eines IT-Audits und bei der Behebung von Mängeln ist es ratsam, eine enge Integration der Projektorganisation mit den etablierten Verteidigungslinien des Unternehmens, bekannt als das Drei-Verteidigungslinien-Modell (LoD – Three Lines of Defense), zu gewährleisten. Ursprünglich im Finanzsektor entwickelt, beschreibt dieses Modell die Verteidigungslinien eines Unternehmens wie folgt:

- **1LoD:** Die direkte Kontrolle wird durch die Geschäftsbereiche und unterstützenden Servicebereiche wie IT und Betrieb ausgeübt.
- **2LoD:** Die Funktion der Informationssicherheitsbeauftragten (ISB) stellt Anforderungen auf, bewertet die Risiken der Informationssicherheit unabhängig und führt eigene Kontrollen zur Überwachung der Umsetzung der Massnahmen der ersten Verteidigungslinie durch.
- **3LoD:** Die interne Revision überprüft die Effektivität des internen Kontrollsystems (IKS) und anderer Risikomanagementprozesse unabhängig von den ersten beiden Linien.

Drei Arten von Projekt- und Programmmanagement: Interne, externe oder hybride Verankerung — Empfehlung

Optionen	Darstellung	Beschreibung
1 **Interne Verankerung** (Insourcing)	Intern: Dep[1] 1, Dep 2, PPM[2]	▪ Einrichtung einer internen Projekt-/Programmorganisation unter der **Leitung** eines **Managers** mit **Erfahrung** im **Projektmanagement** ▪ Erfordert **vollständige Projektpipeline** ▪ **Einstellung von Projektmanagement-Experten** aus der **Industrie** oder **Beratung** ▪ **Ganzjährige Kapazitätsauslastung** muss **gewährleistet sein** ▪ **Günstiger** als Verankerung **mit externen Ressourcen**
2 **Externe Verankerung** (Outsourcing)	Intern: Dep 1, Dep 2, Dep 3; Extern: Dep 1, Dep 2, PPM	▪ Aus **geschäftlicher** und **risikomindernder** Sicht nur **praktikabel**, wenn es **mindestens drei bevorzugte Partner für** die **Rotation** gibt ▪ Interne **Sicherung** von **Betriebs-** und **PPM-Kenntnissen eingeschränkt** ▪ **Doppelte finanzielle Belastung** durch **Kosten** für **Aufrechterhaltung** des internen **Fachwissens** neben den **Kosten** für **externe Experten** ▪ **Erhebliche Kosten**, **Koordinationsprobleme**, **Mangel an internem Management**
3 **Hybride Verankerung**	Intern: Dep 1, Dep 2, PPM; Extern: Dep 1, Dep 2, PPM	▪ **Kapazitätsauslastungslücken** werden durch **externe Experten geschlossen**: - **Generalistische Experten**, **vorausgesetzt**, **intern genügend Fachwissen** vorhanden - **Spezialisierte Projektmanagement-Experten** ▪ **Erfolgsfaktor ist ein definiertes** und **reproduzierbares Liefermodell**, bei dem interne **Experten** für **PPM** zur **Verfügung** stehen und ausgewiesen sind

Quelle: Grey Swan I 1: DEP = Department I 2: PPM = Projekt- und Programmmanagement

Abbildung 18: Drei Formen von Projekt- und Programmmanagement-strukturen

Interne Verankerung (Insourcing)

Die erste Option ist der Aufbau einer internen Projekt-/Programmorganisation, geführt durch eine Führungskraft mit Projektmanagement Erfahrung. Für das Management und die Begleitung von IT-Audits und Mängelbeseitigungsprogrammen ist es entscheidend, dass die Projekt-/Programmorganisation die notwendigen methodischen Kenntnisse vorweist oder diese konsequent ausgebildet werden und zudem in der Lage ist, aufsichtsrechtliche Sachverhalte zu verstehen. Das Modell erfordert eine gesteuerte Projektpipeline und ist vergleichsweise günstig im Vergleich zum Einsatz von Externen. Die Umsetzung könnte durch Anstellung von Ex-Compliance-Experten, -Rechtsberatern, -Unternehmensberatern und -Wirtschaftsprüfern erfolgen. Die Bruchstellen für das Modell sind die Sicherstellung der ganzjährigen Auslastung durch den Einsatz in Projekten aus der Linie, was wiederum die Herausforderung birgt, Verfügbarkeit für ad-hoc anberaumte Audits gegenüber ständiger Auslastung zu balancieren und die Reduktion in der Flexibilität durch dauerhafte oder befristete Anstellungen.

Externe Verankerung (Outsourcing)

Die zweite Option wäre aus betriebswirtschaftlichen und Risikomitigationsgesichtspunkten nur denkbar, wenn mindestens drei, an Rahmenverträge gebundene bevorzugte, Partner, die in einem Rotationsmodell für Spezialprojekte, wie IT-Audits nach XAIT, DORA, IT-SiG usw. und der nachgelagerten Mängelbeseitigung, zur Verfügung stehen. Die Soll-Bruchstelle bei einem Auslagerungsmodell liegt in dem Umstand, dass aufsichtsrechtlich gefordert wird, intern das notwendige Wissen für die Betriebsfähigkeit vorzuhalten, was beim vollständigen Outsourcing nicht gegeben wäre. Eine weitere Problematik ist die finanzielle Doppelbelastung, denn die interne Wissensvorhaltung drückt sich in externen Experten aus. Schlussendlich erzeugt diese Option hohe Kosten, Abstimmungs- und Koordinationsaufwände sowie fehlende interne Verantwortliche.

Hybride Verankerung

Hybridmodelle stellen pragmatischen Ansatz dar

Für die dritte Option werden Auslastungslücken durch externe Experten ausgeglichen. Eine Variante, um personelle Lücken zu schliessen, wäre, unter der Voraussetzung, dass intern ausreichend Expertise vorhanden ist, günstigere und generalistische externe Experten zu beauftragen. Eine zweite Variante des Hybridmodells ist die kurzfristige Beauftragung von spezialisierten Compliance- und Projektmanagement-Experten für Auditsituationen wie z.B. Sonderprüfungen oder komplexere Mängelbeseitigungen. Ausschlaggebend für den Erfolg ist ein Liefer-Modell, in dem die internen Experten für die Audits verfügbar und in der Personalmanagement-Software (z.B. Workday oder Personio) sowie auch die externen Experten entsprechend für den fallbezogenen Abruf gekennzeichnet sind.

Zusammenfassung

Der Unternehmenserfolg wird massgeblich von politischen, regulatorischen und technologischen Herausforderungen bestimmt. Eine professionelle Bearbeitung dieser Herausforderungen ist erfolgskritisch und sollte aus diesem Grund als Projekt oder Programm organisiert werden. Für eine erfolgreiche Umsetzung eines Projektes und Programmes bedarf es erstens methodischer Kompetenz, zweitens Toolunterstützung und drittens Experten für Fachspezifika.

Die Durchführung eines komplexen Programms wurde am Beispiel eines IT-Audits bei Finanzunternehmen und KRITIS-Betreibern dargelegt. Diese sehen sich in Europa einem immer dichter werdenden vertikalen und horizontalen Anforderungskatalog gegenüber und müssen diesen rechtlichen und technologischen Anforderungen genügen.

IT-Audits sind Ausnahmesituationen für die Aufbau- und Ablauforganisation und können zumeist nicht vollständig aus der Linienorganisationen heraus bewältigt werden. Eine besondere Aufbauorganisation für die Vorbereitung und Durchführung des Audits sowie im Nachgang für die Mängelbeseitigung muss fast immer ins Werk gesetzt werden. Unternehmen behelfen sich erfahrungsgemäss mit der Beimischung externer Expertise. Unserer Auffassung nach sollte der Beimischungsgrad pari sein, sodass die aufsichtlich gebotene Expertise weiterhin intern vorgehalten werden kann und Vendor log in-Effekte vermieden werden.

Kritische Infrastrukturen sowie Finanzunternehmen in Europa unterliegen einer Reihe branchenübergreifender regulatorischer Standards wie NIS2, CER, CRA, DSGVO und DORA. Diese umfassenden Anforderungskataloge führen zu einer Zunahme von IT-Audits bei einer grösseren Anzahl regulierter Unternehmen. Die Einführung der NIS2-Richtlinie bewirkt, dass die Anzahl der in Deutschland überwachten Unternehmen von 2.000 auf mindestens 30.000 anwächst. Ab 2025 werden in Europa durch die DORA-Verordnung mehr als 22.000 Finanzunternehmen reguliert; allein in Deutschland fallen über 3.600 Unternehmen des Finanzsektors unter diese Aufsicht.

IT-Audits werden zum „Normalfall“ für ein Unternehmen. Dieses regulatorische Ziel ist gleichzeitig ein sicherheitspolitisches Gebot, da die Sicherheitsorganisation kontinuierlich überprüft und verbessert wird. Eine weitere Digitalisierung überführt das heute als „Sonderprüfung“ bezeichnete IT-Audit zu einem „kontinuierlichen“ Audit. Durch Einhaltung von definierten, erfahrungsbasierten Erfolgsfaktoren für die Auditvorbereitung, -durchführung und Mängelbeseitigung wird das Auditergebnis planbar und mündet seltener in harter Sanktionierung.

Ein „kontinuierliches“ Audit erfolgt über automatisiert zur Verfügung gestellte Messwerte und Schlüssel-Indikatoren. Diese Automatisierung stellt eine konsequente Fortführung von Digitalisierungsstrategien für Infrastrukturen, Anwendungen und Services dar. Ein Audit ist demnach ein weiterer digitaler Service. Dieses digitalisierte Angebot ist mit positiven Rückkopplungseffekten verbunden, denn ein weitgehend automatisiert ablaufender Audit erfordert eine vollständig dokumentierte, Risiko- und lückenlos gesteuerte überwachte Infrastruktur. Aus diesem Blickwinkel gesehen stellt ein IT-Audit keine Betriebsstörung mehr da, sondern ist Werkzeug zur vorgelagerten Steuerung und Überwachung der eigenen Infrastruktur sowie entscheidender Erfolgsfaktor für eine zeitgerechte und effektive Umsetzung der Mängelbeseitigung und ein Wegbereiter einer digital performanten Produktionsplattform, die mehr Raum für das Kerngeschäft lässt.

Quellen

1. Europäischer Rat. (2024). *Sanktionen. Europäischer Rat. Von https://www.consilium.europa.eu/de/policies/sanctions/ abgerufen*

2. Europäische Union. (03.2024). *EU-Sanktionsverfolgung. Europa Analytics. Von* https://data.europa.eu/apps/eusanctionstracker/ *abgerufen*

3. Leisering, K. (02.01.2024). *EQS. Von https://www.eqs.com/compliance-blog/eu-supply-chain-law/ abgerufen*

4. McFarland, A. (11.2023). *Unite AI. Von https://www.unite.ai/oreilly-generative-ai-in-the-enterprise-2023-report/ abgerufen*

5. Gartner. (13.12.2022). *gartner.com. Von https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023 abgerufen*

6. Gartner. (13.12.2022). *Gartner weltweite Markt für Low-Code-Entwicklungstechnologien im Jahr 2023 [Pressemitteilung]. Von https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023 abgerufen*

7. Bank for International Settlements (BIS). (kein Datum). *Basel III: international regulatory framework for banks. Von Bank for International Settlements (BIS): https://www.bis.org/bcbs/basel3.htm abgerufen*

8. BaFin. (18.10.2023). *Rundschreiben 05/2023 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk. Von BaFin: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_MaRisk_BA.html;jsessionid=2278012D386A911119744E387A86E492.internet001?nn=19659504 abgerufen*

9. Europäische Kommission. (2022). *Vorschlag des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zu den Änderungen der Verordnung (EU) 2019/1020. Brüssel: Europäische Kommission.*

10. Europäische Kommission. (2016). *Datenschutz-Grundverordnung. Brüssel: Europäische Kommission.*

11. Europäische Kommission. (2022). *Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnung (EG Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011. Brüssel: Europäische Kommission.*

12. Europäische Kommission. (2022). *Richtlinie (EU) 2022/2464 des europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 537/2014 und der Richtlinien 2004/109/EG, 2006/43/EG und 2013/34/EU hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen. Brüssel: Europäische Kommission.*

13. United Nations. (kein Datum). *United Nations - Department of Economic and Social Affairs Sustainable Development. Von https://sdgs.un.org/goals abgerufen*

14. Global Reporting Initiative. (kein Datum). *Global Reporting Initiative. Von https://www.globalreporting.org abgerufen*

15. U.S. Securities and exchange commission. (25.09.2023). *U.S. Securities and exchange commission. Von https://www.sec.gov/news/press-release/2023-194 abgerufen*

16. Sanction Scanner. (2023). *Financial Crime & Compliance. Von Sanction Scanner: https://sanctionscanner.com/Content/Report/2023-2024-Financial-Crime-and-Compliance-Report.pdf abgerufen*

17. Kröner, A., & Schwarz, D. (18.01.2023). *Finanzaufsicht schränkt Neugeschäft von Fintech Solaris ein. Von Handelsblatt: https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/bafin-finanzaufsicht-schraenkt-neugeschaeft-von-fintech-solaris-ein/28922928.html abgerufen*

18. Handelsblatt. (o. J.). *Smartphonebank: Bafin verlängert Auflagen gegen N26 - Fintech darf weiterhin nur begrenzt wachsen. Von https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/smartphonebank-bafin-verlaengert-auflagen-gegen-n26-fintech-darf-weiterhin-nur-begrenzt-wachsen/29238276.html abgerufen*

19. Deutsche Bank. (09.112020). *Deutsche Bank verkauft Postbank Systems an Tata Consultancy Services. Von Deutsche Bank: https://www.db.com/news/detail/20201109-deutsche-bank-announces-sale-of-postbank-systems-to-tata-consultancy-services?language_id=3 abgerufen*

20. Deutsche Bahn. (2022). *Von Digitalisierungsprojekte und -konzepte im Fokus: https://ibir.deutschebahn.com/2022/de/konzernlagebericht/produktqualitaet-und-digitalisierung/digitalisierung/digitalisierungsprojekte-und-konzepte-im-fokus/ abgerufen*

21. Handelsblatt. (kein Datum). *Handelsblatt. Von Künstliche Intelligenz - Vodafone verbündet sich mit Microsoft: https://www.handelsblatt.com/technik/ki/kuenstliche-intelligenz-vodafone-verbuendet-sich-mit-microsoft/100007448.html abgerufen*

22: Handelsblatt. (01.2024). *Handelsblatt. Von https://www.handelsblatt.com/technik/ki/tech-leitmesse-ces-2024-siemens-verbuendet-sich-mit-amazon-fuer-ki-partnerschaft/100005372.html abgerufen*

23. Market Screener. (2023). *Toshiba. Von Market Screener: https://de.marketscreener.com/kurs/aktie/TOSHIBA-6493713/news/Japan-Industrial-Partners-Inc-ROHM-Co-Ltd-TSE-6963-und-Suzuki-Motor-Corporation-TSE-7269-ha-44894603/ abgerufen*

24. Microsoft. (03.2022). *Microsoft completes acquisition of Nuance, ushering in new era of outcomes-based AI. Von https://news.microsoft.com/2022/03/04/microsoft-completes-acquisition-of-nuance-ushering-in-new-era-of-outcomes-based-ai/ abgerufen*

25. Europäische Bankenaufsichtsbehörde. (01.2024). *Europäische Bankenaufsichtsbehörde. Von Auftrag und Aufgaben der EBA: https://www.eba.europa.eu/deutsch abgerufen*

26. Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung. (6.02.2023). *Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung. Von https://www.eiopa.europa.eu/media/events/joint-esas-public-event-dora-technical-discussion-2023-02-06_en?prefLang=de&etrans=de abgerufen*

27. Europäische Wertpapier- und Marktaufsichtsbehörde. (Januar 2024). *Europäische Wertpapier- und Marktaufsichtsbehörde. Von Überblick: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-securities-and-markets-authority-esma_de abgerufen*

28. Bundesamt für Sicherheit in der Informationstechnik. (2023). *Von Was sind Kritische Infrastrukturen? https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis.html abgerufen*

29. Europäisches Parlament und Rat der Europäischen Union. (2022). *NIS-2-Richtlinie. Brüssel: Amtsblatt der Europäischen Union. Von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&qid=1705010003184 abgerufen*

30. Europäisches Parlament und Rat der Europäischen Union. (2016). *NIS-Richtlinie. Brüssel: Amtsblatt der Europäischen Union.*

31. Deutscher Bundestag. (2021). *Lieferkettensorgfaltspflichtengesetz (LkSG). Berlin: Bundesgesetzblatt.*

32. Dimensional Research, Netenrich. (2021). *Pivoting to Risk-Driven and Proactive Security. Von Dimensional Research: https://netenrich.com/hubfs/web/resources/netenrich-pivoting-to-risk-driven-secops-executive-brief.pdf abgerufen*

Abkürzungsverzeichnis

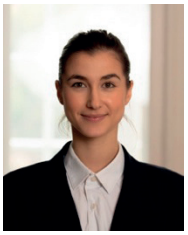
Abkürzung	Bezeichnung
1LoD	Erste Linie der Verteidigung
2LoD	Zweite Linie der Verteidigung
3LoD	Dritte Linie der Verteidigung
BAIT	Bankaufsichtliche Anforderungen an das IT
CER	Critical-Entities-Resilience-Richtlinie
CRA	Cyber-Resilience-Act
CSDDD	EU-Lieferkettenrichtlinien 2022
CSRD	EU-Richtlinie zur Unternehmens-Nachhaltigkeitsberichterstattung
DORA	Verordnung zur Digitalen Operativen Resilienz
DSGVO	Datenschutz-Grundverordnung
DWS	Deutsche Gesellschaft für Wertpapiersparen
ESG	Umweltschutz, Soziales, Unternehmensführung
GRI	Nachhaltigkeitsberichterstattung
IaaS	Infrastruktur als ein Service
ISMS	Managementsystem für die Informationssicherheit
IT	Informations-Technologie
IT-SiG	Informations-technologisches-Sicherheitsgesetz
KAIT	Kapitalverwaltungsaufsichtliche Anforderungen an die IT

Abkürzung	Bezeichnung
KI	Künstliche Intelligenz
KPI	Schlüsselkennzahlen
KRITIS	Kritische Infrastruktur
MaRisk	Mindestanforderungen an das Risikomanagement
NIS1	Netzwerk-Informationssicherheits-Richtlinie 1.0
NIS2	Netzwerk-Informationssicherheits-Richtlinie 2.0
PaaS	Platform als ein Service
PMO	Projekt-Management Office
SaaS	Software als ein Service
SDG	United Nations-Nachhaltigkeitsziele
SDLC	Softwareentwicklungs-Lebenszyklus
SEC	United States Securities and Exchange Commission
sfO	Schriftlich fixierte Ordnung
SME	Fachexperte
ToD	Test-of-Design
ToE	Test-of-Effectiveness
ToI	Test-of-Implementation
VAIT	Versicherungsaufsichtliche Anforderungen an die IT
XAIT	Sammelbegriff für BAIT, KAIT, VAIT, ZAIT
ZAIT	Zahlungsdienstlicheaufsichtliche Anforderungen an die IT

Autoren

Leon Kuhlmann ist Managing Director des Schweizer Think-Tanks Grey Swan. Er verfügt über knapp 10 Jahre Erfahrung in Management- und IT-Beratung. Für seine Kunden hat er in diversen Branchen und Regionen komplexe und umfangreiche (IT-)Transformationsprogramme u.a. auch, durch sein Verständnis für Compliance, mit Bezug auf (IT-)Audits, geleitet und umgesetzt. Zu seinen Kernkompetenzen gehören Programm- und Turnaround-Management.

Julius Düwel ist Manager bei Grey Swan mit einem Master in Management von der IE Business School. Er ist seit mehreren Jahren in der IT-Beratung tätig und spezialisiert auf Programmmanagement, Entwicklung von Risikostrategien und Compliance-Management. Zu seinen Projekten zählen die Leitung von Programmen im Rahmen von 44er Sonderprüfungen gemäss KWG, Business Impact Analysen und Machbarkeitsstudien für Kernbankensysteme.



Pauline Schmidt ist Associate Consultant bei Grey Swan. Sie ist Expertin im ESG- (Environmental, Social & Governance) und Projektmanagement Bereich, mit einem Fokus auf die Förderung nachhaltiger Unternehmensführung. Sie absolvierte ihren Bachelor of Arts in Betriebswirtschaftslehre mit Schwerpunkt Nachhaltigkeitsmanagement an der Hochschule für Technik und Wirtschaft in Berlin.

Tamino Müller ist Fellow Consultant bei Grey Swan. Während seines Studiums an einer Londoner Business School, sammelte er Arbeitserfahrung als Business Analyst und Berater von Fortune 500 Unternehmen. Mit einem Bachelor in Betriebswirtschaftslehre und Schwerpunkt Finanzen, unterstützt er die Silos Risiko-, Finanz-, und Programmmanagement. Seine Erfahrungen umfassen Kreditprozess- und Treasury Optimierungen von Banken.

Über Grey Swan

In einer Ära, die geprägt ist von sich stetig wandelnden geopolitischen und makroökonomischen Herausforderungen, ist die Volatilität zu einer konstanten Begleiterin avanciert. Die Vereinigung dieser vielfältigen Herausforderungen hat die Wahrscheinlichkeit für das Auftreten sogenannter “Grey Swan“-Ereignisse signifikant erhöht. Diese Ereignisse, oftmals von unvorhersehbarer Natur, haben häufig einen tiefgreifenden Einfluss auf Investoren, einzelne Organisationen, Branchen oder ganze Volkswirtschaften.

Unser Ansatz konzentriert sich vor dem Hintergrund des sich entwickelnden Umfelds auf “Strategic Resilience“ – strategischer Handlungsfähigkeit. Wir bieten Expertenberatung in der komplexen Geschäftswelt von heute mit einem vielseitigen und sorgfältig ausgearbeiteten Dienstleistungsportfolio. Unsere Beratungsdienstleistungen konzentrieren sich auf die Bewältigung von Herausforderungen im Bereich Risiko, Compliance, Technologie und Transformation. Dies erfolgt durch die konzeptionelle Gestaltung bestehender Risikomanagementstrukturen, die Optimierung finanzieller Funktionen, die Lösung technologischer Hindernisse sowie die strikte Einhaltung regulatorischer und rechtlicher Compliance-Standards. Weiterhin tragen wir zur Steuerung komplexer Programme bei, um unseren Kunden die Gewährleistung ihrer “Strategic Resilience“ zu ermöglichen.

Haftungsausschluss

Grey Swan Management AG
Baarerstrasse 52
6300 Zug | Schweiz
www.greyswan.ch
Office: +41 43 505 23 22
Kontakt: ch.office@greyswan.ch

April 2024