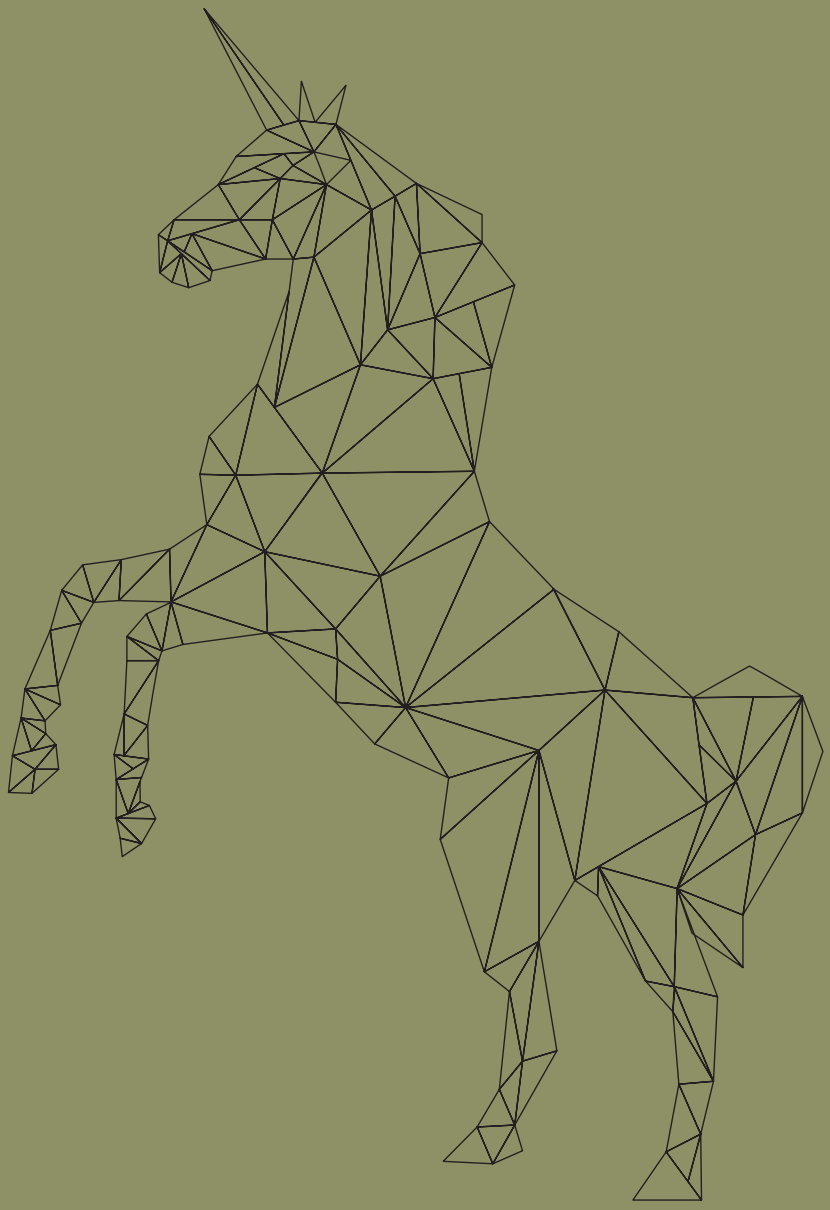
Whitepaper
Operational Due Diligence: Der smarte Weg zur Bewertung
von M & A-Deals in den Bereichen Technologie und Infonomics

How to catch a unicorn! From Risk to Business



audius

audius

Willkommen

Vor fünf Jahren haben wir begonnen, audius-Klienten mit Methoden und Metriken zu unterstützen, um deren operationelle Risiken zu reduzieren und gleichzeitig die operationelle Sicherheit zu verbessern. Entstanden ist ein umfassendes Paket an passgenauen Modulen und Praktiken, das wir heute unseren Kunden im Rahmen des kontinuierlich wachsenden Bereichs „Security and Audit Services“ erfolgreich anbieten.

Unsere Methodik hat sich aus unserem tiefen Wissen heraus entwickelt, das wir über die letzten 25 Jahren hinweg aus zahlreich durchgeführten technischen Tests und Analysen gewonnen haben. Über diesen langen Zeitraum – ein ganzes Zeitalter in der Technologie-Entwicklung- - konnte audius die technischen Erkenntnisse fortwährend schärfen und zeitgleich sicherstellen, dass die aktuellen, operationellen Anforderungen fest im Blick bleiben. Heute nutzen Branchenführer wie auch Investoren auf der ganzen Welt unsere Dienstleistungen, um ihre strategische und operative Entscheidungsfindung zu komplettieren und abzusichern. Die Entscheidungsprozesse, die sich mit Fusionen und Übernahmen – M&A Deals – befassen, sind dabei besonders kritisch.

Unsere M&A Due Diligence trägt ohne Zweifel durch umfangreiche und erprobte Mechanismen entscheidend zur Risiko-Reduzierung bei. Wir sind stolz darauf, unseren Kunden eine neue Perspektive und einen umfassenden Blick auf mögliche neue Deals zu eröffnen.

In diesem Whitepaper erfahren Sie, wie wir einen Mehrwert auch für Ihren M&A-Prozess generieren.

Matthias Kraft
Vorstand

Joerg Simon
Bereichsleiter Security & Audit Services

audius erweitert die Due Diligence um einen neuen Assessment-Channel

From Risk to Business
Bessere Entscheidungsfindung für Infonomics M&A Deals

audius operational Due Diligence	Traditionelle M&A Bewertung: Rechtliche und finanzielle Due Diligence
Analyse und Bewertung von Non-capital Assets mit der **Loss-Control-Methode**	Wertvolle Expertise in der Bewertung von Vermögenswerten Keine Expertise in der Bewertung von Non-capital Assets im Infonomics Umfeld
Proof of Concept, Ideen, IP, Code, Produkte Früherkennung von Bedrohungen und deren Auswirkungen Reduziertes Risiko von Fehl-investitionen Entscheidungen auf der Grundlage von Fakten, nicht von Annahmen Erfordert die Orchestrierung neuer Expertenfähigkeiten Liefert Kontext, Vergleichbarkeit und Messbarkeit	Kritisch für jedes M&A-Geschäft Risiko, versteckte Deal-Breaker nicht zu erkennen

The New Diligence

Wie erfährt man, was zum Game-Changer wird? Oder auf welches Pferd man setzen soll?

Die Technologie verändert sich schneller, als wir denken können. Und sie treibt das Geschäft auf der Informationsautobahn voran. Deshalb wollen Investoren die Ersten sein, die das nächste „große Ding" entdecken. Ihr Fokus liegt auf intelligenten Technologien wie IoT, Automatisierung, KI und Digitalisierung.

Als Mitreisende auf dem sich ständig verändernden Gebiet der Infonomics - der Monetarisierung von Informationen sowie der daraus resultierenden Intelligenz - müssen Investoren jedoch in der Lage sein, über den Tellerrand hinauszublicken. Vor allem bei der Beurteilung des Potenzials einer Technologiefirma, die ihr Interesse geweckt hat.

Hier kommen Methoden, die nicht für Smart-Tech maßgeschneidert sind, schnell an ihre Grenzen. Die „klassischen" Due-Diligence-Ansätze für Mergers & Acquisitions (M&A) allein reichen für eine faire und effiziente Bewertung einfach nicht aus.

Warum?

Aus dem simplen Grund, dass Tech-Startups keine klassischen Assets haben und sich generell nicht in gewohnten Bahnen bewegen.

Tech ist ein Formwandler, der sich nicht an traditionelle Regeln hält. Die Wahrscheinlichkeit, dass Tech-Startups für einen längeren Zeitraum die Gewinnzone nicht erreichen, ist hoch. Die siegreiche Wette ist in den meisten Fällen die Idee, der Code, die Information Assets, der Proof of Concept oder die zu erwartenden zukünftigen Ergebnisse des Unternehmens und nicht die herkömmlichen Bilanzkriterien.

Es überrascht daher nicht, dass „klassische" Methoden, so effektiv sie auch sein mögen, bei der Beurteilung eines M&A-Kandidaten aus dem Technologiebereich nicht das ganze Bild aufzeigen. Oder sie sorgen sogar für eine noch größere Überraschung. Traditionell werden hochqualifizierte Beratungsfirmen und Anwälte herangezogen, um den Zustand eines Unternehmens sowie seinen rechtlichen und finanziellen Aufbau zu überprüfen. Aber wenn der wahre Wert eines Startups in seinem geistigen Eigentum (IP) liegt, muss der Umfang der Prüfung erweitert werden. IT-Infrastruktur und -Sicherheit sind dann nicht mehr nur ein operatives Thema unter vielen anderen. Sie sind plötzlich in den Mittelpunkt des Interesses gerückt.

Betrachten Sie ein - fiktives - Fintech-Startup mit eindrucksvollen Perspektiven aufgrund seines einzigartig effektiven Benutzerdaten-Management-Ansatzes. Stellen Sie sich ebenfalls vor, dass Sie es sind, der die Bewertung im Sinne der klassischen Due Diligence durchführt.
Ein Startup mit fast keinem Umsatz, aber dennoch mit einer äußerst wertvollen, aber auch gleichzeitig anfälligen IP - was könnte da alles schieflaufen?

Eine ganze Menge natürlich. Deshalb darf die Prüfung nicht nur die Bilanz, die Bücher und dergleichen umfassen. Zusätzlich zur klassischen Due Diligence ist es unerlässlich, potenzielle Produktrisiken, wie z.B. IP-Probleme, und unternehmensbezogene Risiken, wie z.B. Infrastrukturschwächen, zu identifizieren. Um zu beurteilen, ob ein Geschäft abgeschlossen werden soll, wird ein Technologieinvestor daher nach Möglichkeiten suchen, die Due Diligence zu modernisieren und zu einer „New Diligence" auszuweiten. Mit anderen Worten: Ein Upgrade durchzuführen!

Und genau das macht audius seit einigen Jahren erfolgreich. Bereits über ein Jahrzehnt hinweg hat audius ein Instrumentarium zur besseren, umfassenden Entscheidungsfindung entwickelt, die **Loss-Control-Methode**.

Einzigartig in ihrer ganzheitlichen Orchestrierung von tiefgreifenden Überprüfungen über alle operativen Kanäle hinweg, liefert sie Kontext- und Geschäftsinformationen in einem zuverlässigen, ergebnisorientierten Prozess. Der Ansatz erreicht ein optimales Gleichgewicht zwischen angemessenen operationellen Maßnahmen und der Einhaltung von Standards, Gesetzen und Vorschriften. audius hat Metriken zur Bewertung betrieblicher Risiken bei Fusionen und Übernahmen entwickelt, die Ihnen helfen, die Informationstechnologie sinnvoll zu nutzen, Sicherheit und Risiko einzuschätzen, die Vertrauenswürdigkeit zu beurteilen und die gesammelten Informationen in einen praktischen Kontext zu setzen. In den letzten Jahren haben immer mehr Investoren unser System genutzt, um M&A-Aktivitäten zu rationalisieren und schneller zu effektiven Ergebnissen zu kommen.

Unsere Mission **„From Risk to Business"**: ein kontinuierlicher Prozess zur Bewertung des operationellen Risikos, der Implementierung von Maßnahmen und Prozessen – und des Generierens von Erfolg. Das Ergebnis ist dreigeteilt:

- **Realistischere Bewertungen** durch Transparenz

- Zukünftige Investitionen und damit verbundene **Risiken werden frühzeitig aufgedeckt**

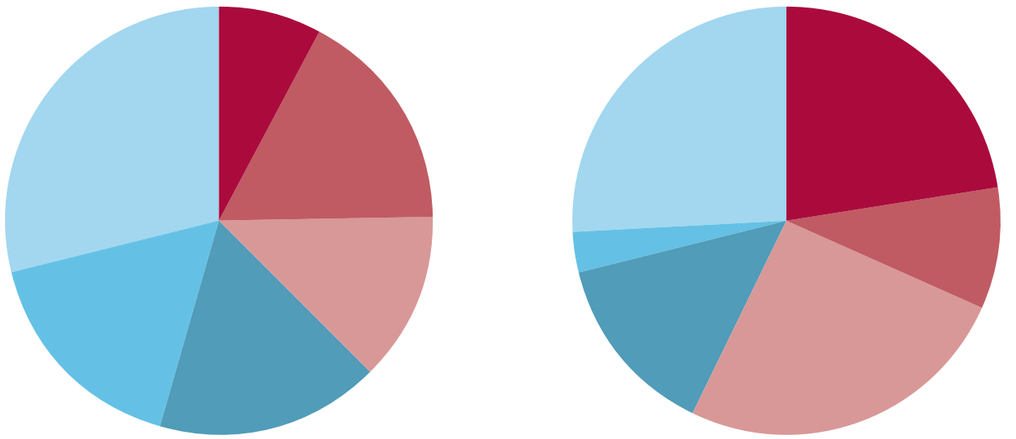
- **Hochstapler werden sofort entlarvt**, indem die Diskrepanz zwischen Marketing und Realität direkt freigelegt wird

Wer auf die Jagd gehen will, muss sich zuerst mit dem Gebiet vertraut machen.

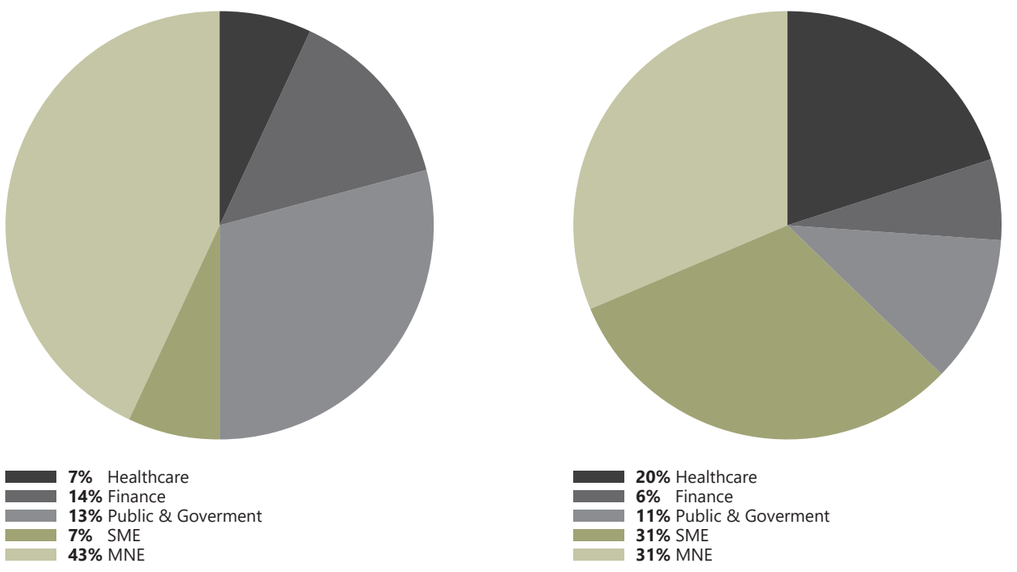
Und was die M&A-Landschaft betrifft, hat sich das Gebiet in den letzten Jahren grundlegend verändert. So hat sich beispielsweise bei den Motiven der audius-Kunden für den Einsatz unseres operativen Due-Diligence-Ansatzes eine deutliche Verschiebung ergeben. Statistiken, die wir aus über 200 Security- und Audit-Projekten von 35 Klienten erstellt haben, zeigen, dass operative Due-Diligence-Projekte zur Unterstützung der M&A-Bewertung und Entscheidungsfindung in den letzten drei Jahren um 15% zugenommen haben.

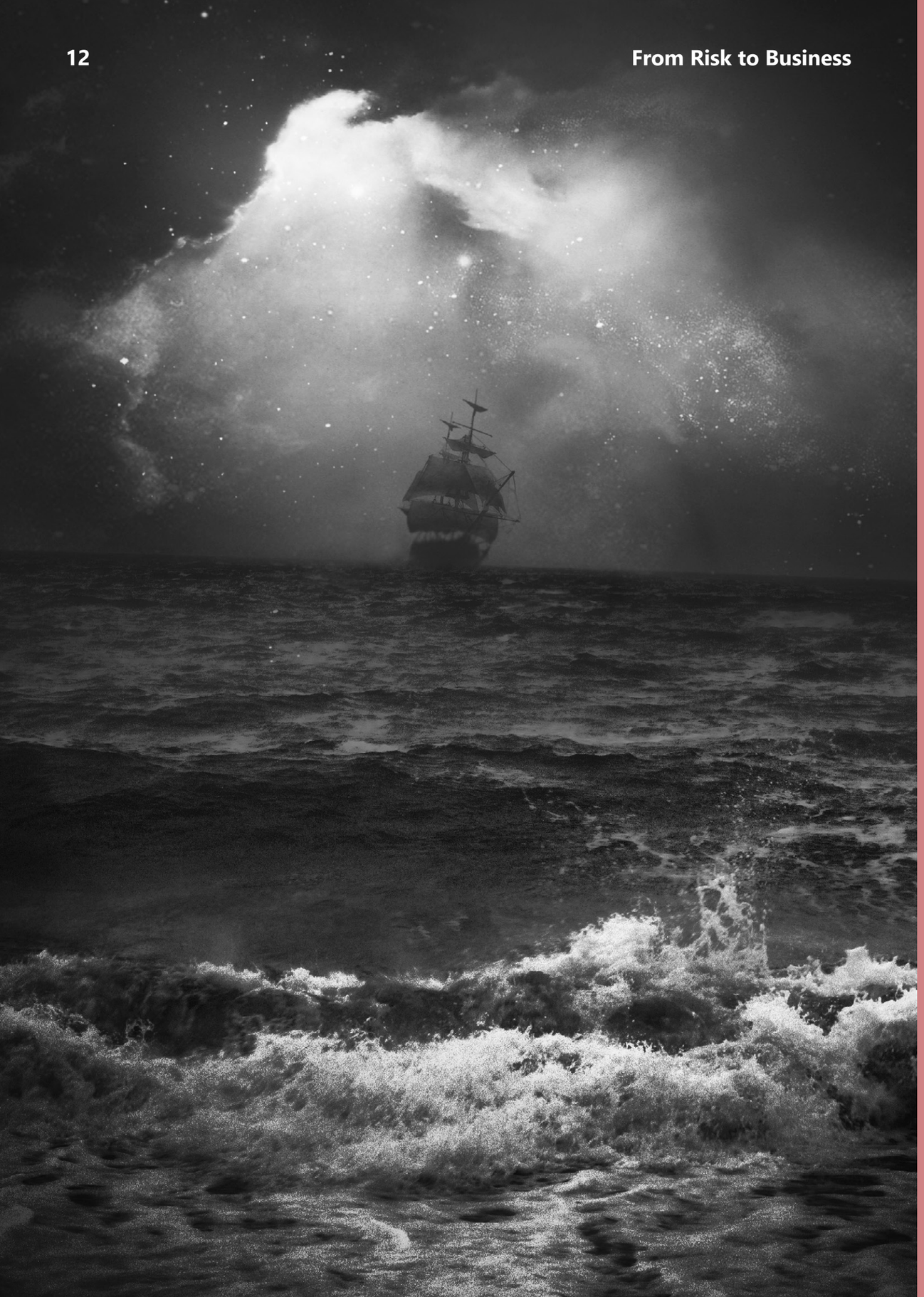
Die audius Security- und Audit-Methoden waren schon immer zur Evaluierung strategischer Ansätze, zur Bewertung von Kontrollverlust, Sicherheit und operationellem Risiko branchenübergreifend anwendbar. In den letzten 24 Monaten haben sowohl kleine und mittlere Unternehmen (KMU) als auch multinationale Unternehmen (MNU) zunehmend in die Digitalisierung investiert, indem sie innovative Unternehmen und Start-Ups übernommen haben. Im KMU-Segment jedoch ist die Anzahl der Projekte am stärksten gewachsen - von 7% auf 31%. Ebenfalls gewinnen M&A-Aktivitäten auch für kleinere Unternehmen immer mehr an Bedeutung. Mit unseren optimierten Angeboten haben diese Unternehmen Zugriff auf hocheffiziente Dienste, die nicht nur schnell, sondern auch erschwinglich sind.

Motives before 2016 → Motives last 3 years



Industry Distribution before 2016 → Industry Distribution last 3 years





From Risk ...

Nicht glauben, sondern wissen.
Und um zu wissen, muss man über den Tellerrand hinausschauen.

Die Due-Diligence-Prüfung, die audius zur Beurteilung von Smart-Tech-Kandidaten durchführt, unterzieht die Unternehmen, ob jung oder etabliert, einer eingehenden technischen Überprüfung, um ihr Innenleben offenzulegen. Dadurch werden versteckte Risiken, mit denen das Unternehmen konfrontiert ist, gleich zu Beginn aufgedeckt und die praktischen Folgen vorhergesagt. Wir definieren Risiko dabei durch drei Elemente: die Bedrohung, ihre Auswirkungen und die Eintrittswahrscheinlichkeit. Der audius-Ansatz konzentriert sich darauf, unbekannte Bedrohungen aufzudecken und zu prüfen, wie wahrscheinlich das Auftreten bekannter Bedrohungen ist.

Solche Bedrohungen können einen **Deal-Breaker** darstellen, wenn sie denn erkannt werden. Bleiben Sie unentdeckt, können sie **extreme finanzielle Schäden** verursachen.

Die folgenden Beispiele aus der Praxis veranschaulichen einige solcher Szenarien, auf die **audius** bei Assessments gestoßen ist und extrapoliert das jeweilige Schadensspotenzial.

RISIKEN AUS DEM PRODUKT-BEREICH

Bedrohung

GEFÄLSCHTES PRODUKT	TECHNISCHE SCHWACH-STELLEN	ELEMENTARER SECURITY-DESIGN FEHLER	ELEMENTARER ARCHITEKUR-DESIGN-FEHLER	TECHNOLOGIE KURZ VOR EINFÜHRUNG VERALTET	RECHTE AN GEISTIGEM EIGENTUM UNKLAR	MANGELNDE SELBSTERKENNTNIS
Die Idee, das Produkt oder eine angegebene Zahl ist nicht echt; es gibt keinen Beweis, dass das Produkt wie behauptet funktioniert Beispiel: Funktionalitäten werden angepriesen, funk-tionieren aber für den User nicht	Software oder Hardware offen für System-Breach Beispiel: Eine Hintertür im IoT-Gerät, die von Angrei-fern ausgenutzt werden kann	Beispiel: Veraltete oder gefährliche Chipsätze, wie z.B. solche, die mit gefähr-lichen Funkwellen arbeiten Leichte Zugänglichkeit, wie z.B. ein Neustart von einem normalen USB-Stick aus	Beispiel: Code oder Infra-struktur sind nicht skalierbar	Chipsätze sind ausgeliefert, werden aber demnächst vom Hersteller nicht mehr unterstützt Veraltete IoT-Hardware bereits beim Kunden integriert	Beispiel: Es ist nicht eindeutig, wem die Idee gehört. Missbräuchliche Verwendung von offenem Quellcode (Open Source Code) oder gestohlenem Code. Nutzung von Biblio-theken, die keine kommer-zielle Verwendung oder ge-schützte Weiterentwicklung erlauben.	Beispiel: Der angebliche USP ist doch nicht einzig-artig, so dass das „in einem Keller" ent-wickelte Produkt bereits in einer größeren und besseren Form existiert.
Reifegrad des Produkts und Benutzer- oder Produkt-zahlen sind niedriger als erwartet Teure Fehlinvestition	Non-compliance führt zu Rufschädigung (Dies kann häufig mit Geld behoben werden)	Haftungsgrund Man muss bei Null beginnen Hoher finanzieller Schaden Irreparabel, deshalb ein Deal-Breaker	Nicht-funktionale Fehler in der Wartbarkeit Geringe Skalierbarkeit und Benutzerfreundlich-keit Zusammenbruch des Geschäfts	Viel vermeidbare Klein-arbeit Gesamtes Framework zerbricht Hohe Ausgaben wegen erheblicher Wartungs-kosten	Zukünftige Verpflichtungen und Verbindlichkeiten Unlösbare Abhängigkeiten Rechtliche Verwicklungen und Lizenz-Abhängigkeiten Kann eine Neuentwicklung erfordern	Große Investitionen sind erforderlich, um etablierte Produkte am Markt zu überholen Investor ist gezwungen aufzuholen

Mögliche Auswirkung

Risiken aus dem Unternehmens-Bereich

Bedrohung

NIEDRIGER „BUS-FAKTOR“	PERSONALKNAPPHEIT	UNSICHERE ARBEITSBEREICHE, DESOLATE INFRASTRUKTUR	ZWEIFELHAFTE GERÄTEHERKUNFT	LÜCKEN IM PROZESS, SCHLECHTES MANAGEMENT	„DÜSTERE“ CLOUD-UMGEBUNG
Der ‚Nerd in Ihrem Keller‘ ist tatsächlich einzigartig und wenn er je von einem Bus überfahren wird, ist das Spiel aus Mit anderen Worten ausgedrückt: es gibt keinen Informationsaustausch zwischen den Mitgliedern des Kernteams, weil nur eine Person den Inhalt überhaupt versteht	HR hat geringe Kapazität	Unzureichende oder fehlende Sicherheitskontrollen, z.B. in einem gemeinsamen Arbeitsbereich, z.B. schwaches Passwort für den Datenbank-Zugriff Berechtigungsnachweise liegen weit offen	Die Software ist nicht firmeneigen, was dazu führt, dass quasi jeder sie besitzen könnte	Beispiel: Kein Sicherheits-Profiling für eine Funktionalität Fehlende Veränderungskontrollen in der Hardware Logistik	Ihre Cloud sieht in Bezug auf Sicherheit nicht den Silberstreif am Himmel und lädt Angreifer ein, Sie zu „pwnen“, wie es im Internet heißt (d.h. sie zu übernehmen, sie zu beherrschen)
Projekt in der Schwebe, wenn es überhaupt überlebt Laufende Arbeiten im Schneckentempo Endgültiger Kontrollverlust	Kein Geld für Neueinstellungen → langsamer oder gar kein Fortschritt → Umsatzrückgang → noch weniger Geld	Unternehmens-Assets sind verwundbar und IP ist offengelegt, bevor die Tinte trocken ist Code, der als IP verkauft wird, landet in einem öffentlichen Repository Endet in einem Public-Relations-Alptraum	Digitale Assets mit hohem Kontrollverlust Datendiebstahl	Ressourcenverschwendung durch Ineffizienz Aktualisierungsbedarf in der Lieferkette, Austausch und Sicherheit; dann Neueinführung Hardware-Hintertüren für Dritte	Digitale Assets mit hohem Kontrollverlust Verlust von IP, der nur sehr kostspielig zu beheben ist Datenpannen hinsichtlich der Datenschutz-Grundverordnung (DSG-VO) mit verbundenen Folgeschäden

Mögliche Auswirkung

… to Business - Die Methode

Jetzt zum Kern der Sache.

Wie können wir diejenigen Bedrohungen aufspüren, die ein Unternehmen in Gefahr bringen, die aber bei einer normalen Überprüfung übersehen worden wären? Denken Sie einfach an ein M&A-Audit, das Sie bereits kennen, allerdings ergänzt durch eine gut eingestellte Lupe, die neue Auditbereiche eröffnet.

Keine Frage, Fusionen und Übernahmen sind anspruchsvolle, langwierige Prozesse. Dem noch mehr Komplexität hinzuzufügen, ergibt wenig Sinn. Deshalb hat audius eine Methode entwickelt, die die Tiefen auslotet, ohne die ohnehin schon mühsamen Prozesse mehr als notwendig zu belasten. Die **Loss-Control-Methode** - sozusagen unser gut justiertes Vergrößerungsglas - ist verlässlich. Sie ist erprobt und bewährt und dabei einzigartig am Markt.

Die heute von unserem Security & Audit-Service Bereich angewandte Methode ist in Verbindung mit unserem Engagement innerhalb eines weltumspannenden Ökosystems von IT- und Security-Communities entstanden. Ziel dabei ist, die Erfahrung mit Technologie weltweit zu verbessern. Als Teil dieser Communities wurde audius zum zentralen Akteur auf diesem Gebiet – insbesondere bei kniffligen Penetrationstests (in die nur Insider Einblick bekommen).

Im Rahmen unserer Beiträge in Form von Forschung und weiterer Unterstützung, unter anderem für das Fedora-Projekt, Alpine Linux, ISECOM, home-assistant.io, explIoT, nullcon, null-community und hardwear.io begann die **Loss-Control-Methode** Gestalt anzunehmen.

Vor dem Hintergrund unserer seit über 10 Jahren andauernden Erfahrung im Bereich Security & Audit Service hat die Loss-Control-Methode audius in die Lage versetzt, Ergebnisse schnell und mit vertretbarem Aufwand zu liefern. Darüber hinaus haben wir sichergestellt, dass unsere Due-Diligence-Talente, sprich unsere Mitarbeiter, mit allen notwendigen Fähigkeiten ausgestattet sind, um M&A-Projekte für Investoren weltweit erfolgreich durchzuführen. Tatsächlich ist die effiziente Orchestrierung von Fachwissen

Heute decken wir das gesamte Spektrum eines technischen Checks mit einem **4 Channel Assessment** ab:

Spectrum Channel – SpecOps
(Wireless)

Human Channel – HumOps
(Processes, Compliance)

Communication Channel – CommOps
(DataSec/TelSec/AppSec/NetworkSec)

Physical Channel – PhysOps
(Building, Facility, Hardware etc.)

einer unserer wichtigsten Wettbewerbsvorteile. Die Überprüfungen befähigen dazu, Entscheidungen auf Basis von nachprüfbaren Fakten zu treffen und nicht bloß aufgrund von Mutmaßungen, Best Practice Ableitungen oder schlicht aufgrund eines Gefühls, indem sie ein Dreiergespann aus **Kontext, Vergleichbarkeit und Messbarkeit** liefern.

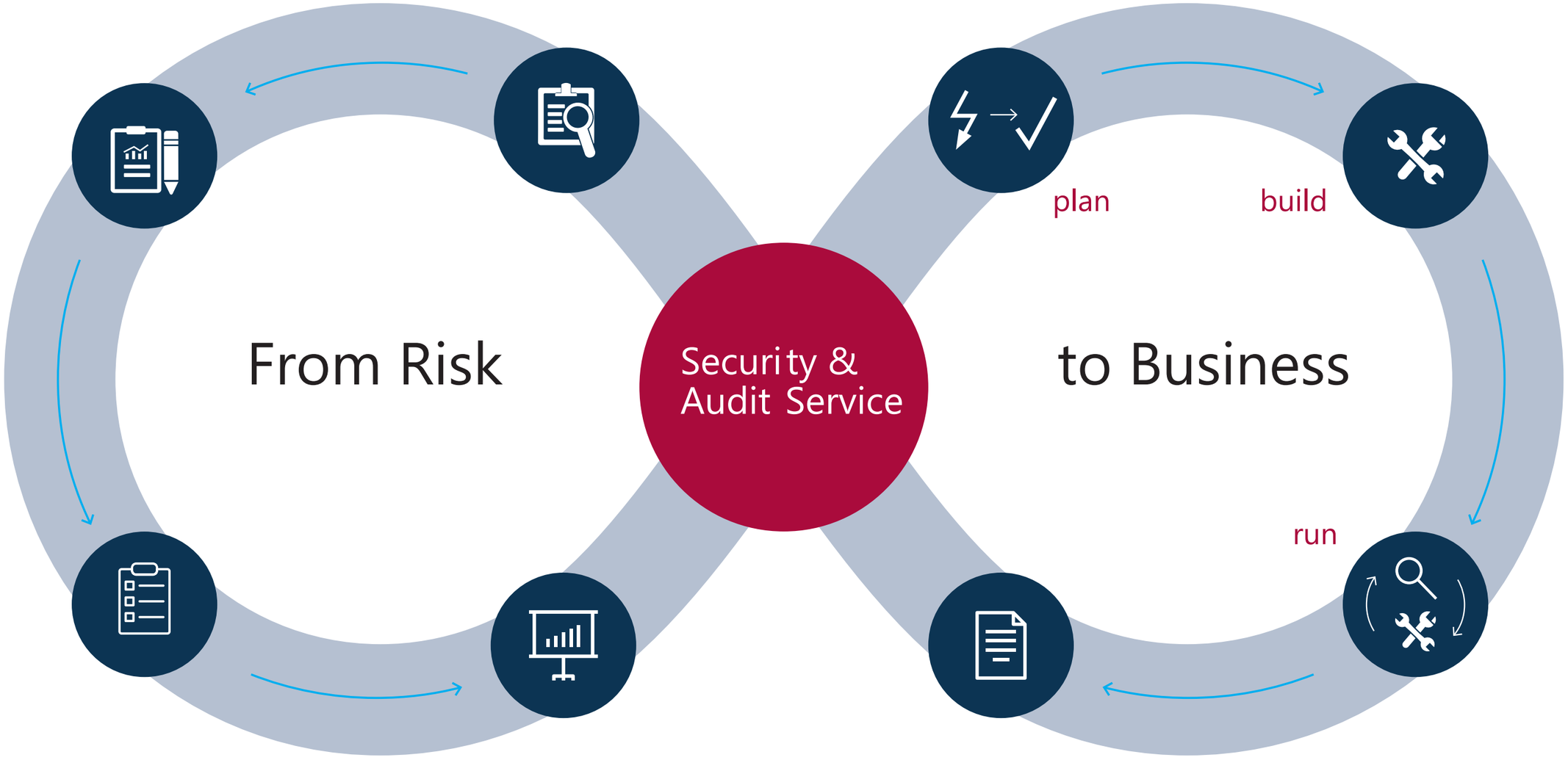
Wir haben schnell gelernt, dass selbst die extremsten Entdeckungen - Erkenntnisse, die uns wortwörtlich umgehauen haben - ohne einen angemessenen Kontext und ohne die Möglichkeit gemessen oder verglichen werden zu können, nur von sehr geringem Wert sind. Und anstatt uns nur auf IT-Fragestellungen zu beschränken, haben wir Penetrationstests, Infrastruktur-Reifegradbewertungen, Compliance Management, Prozessmanagement und Risikomanagement zu einer einzigartigen Methode zusammengeführt. Als Ergebnis all dieser Arbeit wurde die Loss-Control-Methode geboren. Sie wurde zum Kern unserer Mission und half uns gleichzeitig, unserem Leitsatz **„From Risk to Business“** treu zu bleiben. Obwohl es schwieriger war, als wir anfangs erwartet hatten, gelang es uns schließlich, der alles entscheidenden Frage auf den Grund zu gehen: „Was bedeutet das für Ihr Unternehmen?“

Risk Assessment / OpRisk Management
Know what stops your business operations, know what harms your reputation! Know where to put your money first!

Structural Analysis / OpSec
Know your operational security! Know what is where! Know your trust! Know your controls! Know functional & non-functional requirements!

Risk Treatment / Actionplan
Design perfect operational security! Balance your assets, trusts, controls & limitations!

Improve & Mitigate
Implement technical & process measures to improve current operational security!



Compliance Management
Know your legal framework! Know which law, standard or regulation to follow & which could be a threat to the business!

Process Organization
Know how processes deal with the human factor in security!

Security Test & Audits
Make the reality check! Pentests, infrastructure maturity audits & technical assessments as catalyst to learn how your controls need to work!

Monitor
Continuously measure / manage operations, security, limitations & trusts!

Konzeptionell basiert die Loss-Control-Methode auf einem Ansatz, der den Kontrollverlust eines Unternehmens für bestimmte Bewertungseigenschaften und Bewertungskanäle evaluiert.

Die Methode verwendet objektive Metriken und liefert somit vergleichbare Ergebnisse. Dies wiederum ermöglicht es dem Analysten, die Diskrepanz zwischen dem Ist-Zustand und der idealen „Verlustkontrolle“ zu definieren. Erst nachdem eine Lücke identifiziert wurde, kann diese kontrolliert geschlossen werden. Die Methode wurde erweitert und verfeinert, so dass sie eine Vielzahl von funktionalen und auch nicht-funktionalen Anforderungen an den Betrieb umfasst; „funktional“ bezieht sich auf die Kernfunktionalität, „nicht-funktional“ auf die Eigenschaften des Geschäftsbetriebs als Ganzes. Diese nicht-funktionalen Anforderungen wie Belastbarkeit, Vertraulichkeit oder Wartbarkeit sind natürlich auch für Unternehmen von großer Bedeutung. Mit dieser Methode liefert audius Einblicke, Kennzahlen und Transparenz in Bezug auf operationelle Risiken, Sicherheit und Einsatzbereitschaft - abgekürzt OpRisk, OpSec und OpReadiness - für alle Bewertungskanäle: effizient, objektiv und schnell.

→ **OpRisk (operationelles Risiko):**
Unter operationellem Risiko versteht man die Wahrung der Geschäftskontinuität und wie ein Unternehmen oder Produkt in die Lage versetzt werden kann, um hohe Lasten schnell zu bewältigen und mit Notfallsituationen wie Angriffen und jeglichen Katastrophen fertig zu werden. Insbesondere nicht-funktionale Anforderungen wie Verfügbarkeit, kurzfristige Skalierbarkeit und Belastbarkeit werden analysiert, berücksichtigt und gemessen.

→ **OpSec (operationelle Sicherheit):**
Die operationelle Sicherheit liefert Informationen über den Zugang und den Umgang mit Geheimnissen und Informationen und wie diese gesichert sind. Konkret liegt der Schwerpunkt auf nicht-funktionalen Anforderungen wie Vertraulichkeit und Änderungskontrolle.

→ **OpReadiness (operationelle Einsatzbereitschaft):**
Die operationelle Einsatzbereitschaft sammelt Informationen darüber, wie der Geschäftsbetrieb verwaltet, dokumentiert und für die Zukunft vorbereitet wird. In diesem Bereich sind nicht-funktionale Anforderungen wie Effizienz, Wartbarkeit und langfristige Skalierbarkeit von besonderer Bedeutung.

Success Story by

ebmpapst

We would like to illustrate an instance of how operational due diligence allowed a leading company secure its ends swiftly for its startup offshoot. Recently, ebm-papst, a world market leader for energy-saving fans and motors, used its offshoot ebm-papst neo to gain a stake in two strong international partners and allow for rapid transfer of technology.

Thomas Sauer
Managing Director at ebm-papst neo GmbH & Co. KG

The decisions concerning the investments were supported by concrete facts made evident by the operational due diligence audius performed. „We managed to integrate the broad base of special knowledge and expertise of audius into our decision making process and have almost instantly gathered insights, we would not have been able to get without", states Thomas Sauer, Managing Director at ebm-papst neo GmbH & Co. KG.

With a thorough understanding of the company's needs, we concentrated on the specific requirements of a highly virtual startup where the team is scattered across continents. Moreover, we conducted assessments on site in Europe and Asia. audius delivered its intelligence in time and on budget, without straining too many company resources. The result was a useful and valuable addition to the to-do lists from legal and financial due diligence. Moreover, the products provided by the startups had been refined through the value added by audius.

We are happy to report that we received extremely positive feedback from the company. We were told audius has done an incredible job and that its results and metrics were invaluable in the decision-making process.

Das perfekte Zusammenspiel der Kompetenzen

Data Protection
Holger Zürn
and Team

Methods, Metrics and Intelligence
Steffen Lier
and Team

Processes and Management Systems
Juliane Scholz
and Team

IoT, Cloud & Innovation
Stephan Traub
and Team

Standards & Compliance
Markus Biche
and Team

Security & Penetration Testing
Jens Mücke
and Team

Infrastructure
Michael Mederer
and Team

Physical Risk
Markus Biche
and Team

Open Source & Open Standards, Code-Licensing
Jan Berens
and Team

Warum audius?

Auf diese Frage gibt es viele Antworten: jahrzehntelange Erfahrung, State-of-the-art-Technologien, zertifiziertes Qualitätsmanagement und preisgekrönte Innovationen. Letzten Endes läuft aber alles auf eines hinaus: unsere Fähigkeit zuzuhören. Der Fokus auf die konkreten Bedürfnisse von Kunden ist aus unserer Sicht die Grundlage des Erfolgs – des Erfolgs der Kunden und auch unseres eigenen.

Unsere Unternehmensgeschichte ist eine ununterbrochene Wachstumsstory. Gegründet im Jahr 1991 als Software-Haus mit vier Mitarbeitern, hat sich audius seither zu einem führenden mittelständischen IT- und Softwareunternehmen entwickelt. Heute haben wir etwa 500 Mitarbeiter, 17 globale Standorte und etliche Tochterunternehmen. Zu unserem Kundenstamm gehören Organisationen aus allen Branchen und Segmenten, vom Mittelstand über globale Konzerne bis zu öffentlichen Institutionen.
Was sich in den vergangenen Jahrzehnten allerdings nicht geändert hat, ist unser unternehmensweiter Teamgeist. Wir sind nach wie vor ein inhabergeführtes Unternehmen mit schlanken Strukturen und schnellen Entscheidungswegen. Aus diesem Grund ist audius in der Lage, maßgeschneiderte Lösungen effizient und schnell zu liefern. Frei nach der Redensart: Not the big ones beat the little ones, but the fast beat the slow.

Die gleichen Werte veranlassten uns auch zur Entwicklung unserer operativen Due-Diligence-Dienstleistungen, einer Lösung, die speziell auf Mergers & Acquisitions-Deals im Bereich Infonomics und Startup zugeschnitten ist: Wir wollten dynamische Unternehmen dabei unterstützen, bei ihrer M&A-Due-Diligence-Prüfung noch einen Schritt weiter zu gehen. Technisches Know-how, absolute Hingabe an die Kundenbedürfnisse, einzigartiger Ansatz mit nachgewiesener Erfolgsbilanz - diese typischen audius-Merkmale zeichnen unsere Operational Due Diligence Services ebenso aus wie die zahlreichen anderen Angebote unseres Unternehmens.

Unser breitgefächertes Angebot umfasst:

- **Hochwertige IT-Dienstleistungen, Beratung und Cloud-Lösungen**
- **CRM-Systeme für Kunden, Service und Vertrieb**
- **Mobile Unternehmensanwendungsplattform für alle Unternehmenssektoren und -bereiche**

audius
Mercedesstr. 31
71384 Weinstadt
www.audius.de

Kontakt:
Joerg Simon
Bereichsleiter Security & Audit Services
joerg.simon@audius.de
+49 7151 36900 337

Stand Oktober 2020

audius

30 years of running IT for people