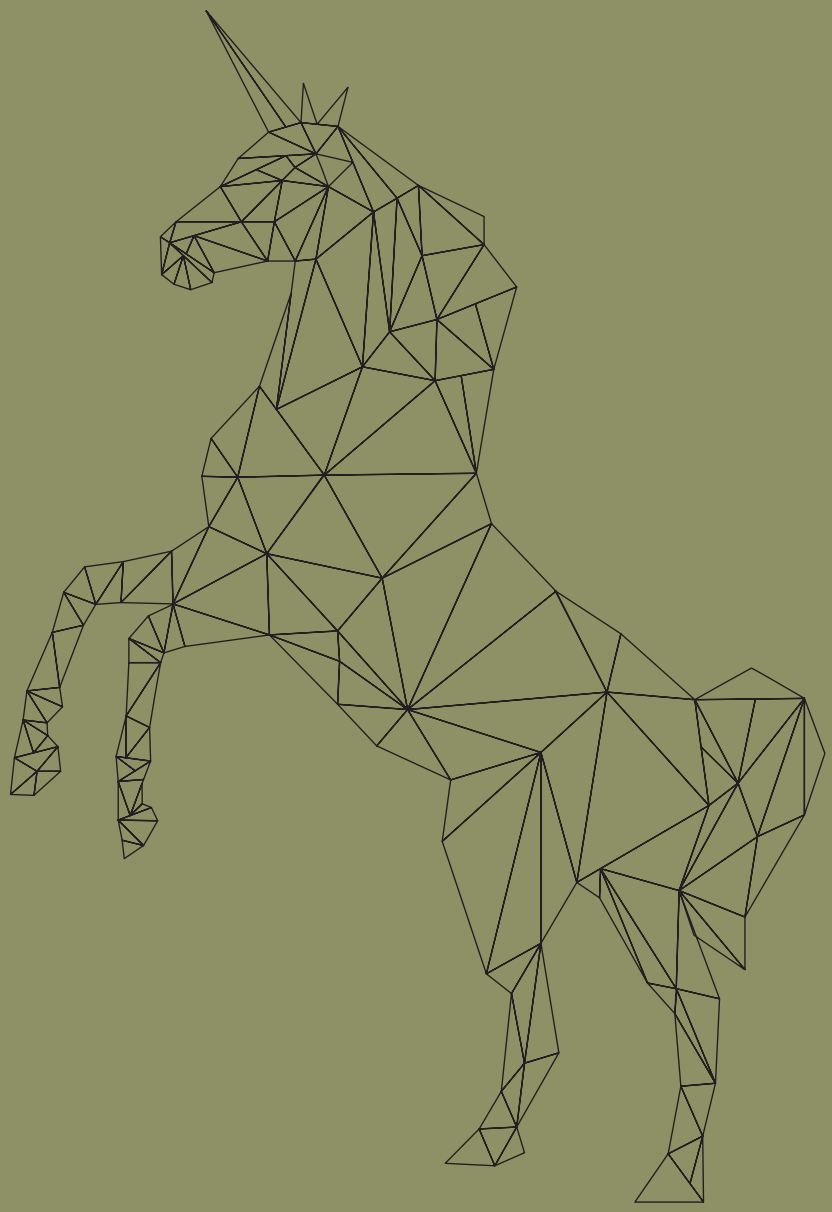
Whitepaper
Operational due diligence: The smart route to assessing M&A deals in tech and infonomics

How to catch a unicorn! From Risk to Business



audius

Welcome Note 4
Summary 6
Introduction: The new diligence 8
The hunt 10
From Risk to Business
From Risk ... 12
Risks from Product Cluster 14
Risks from Company Cluster 16
... to Business – The Method 18
Success Story by ebm-papst 24
Mastering the orchestration of skills 26
Why audius 28
Index 30

audius

Welcome

Five years ago, the two of us came together to support audius clients with methods and metrics that can curtain their operational risks and enhance operational security. The comprehensive module of these practices is what we today offer through our thriving business division called ‚Security and Audit Services'.

Our methodology is derived from acute business intelligence gleaned from over a quarter-century of deep technical testing and analysis. This is aeons in technological time, throughout which audius has constantly sharpened its technical insights while ensuring they remain firmly rooted in actual operational needs.

Today industry leaders and investors around the world seek out our services to contour their strategic and operational decision-making. Critical among such decisive processes is the business end that deals with Mergers and Acquisitions.

The M&A due diligence, without doubt, already has extensive risk reduction mechanisms in place. And we are proud that our service is in great favour by clients who want to achieve fresh perspectives on prospective deals and view them in totality.

In this paper, we set out how we add value to the M&A process.

Matthias Kraft
Board Member

Joerg Simon
Division Director Security & Audit Services

audius expands due diligence with a new assessment channel

From Risk to Business: Better decision-making for infonomics M&A deals

audius operational due diligence	Traditional M&A business evaluation: legal and financial due diligence
Analysis and evaluation of non-capital assets with the **Loss Control Method**	Highly valuable expertise in capital assets evaluation Not equipped to evaluate non-capital assets in the infonomics space
Proofs of concepts, ideas, IP, code, products Early threat and impact detection Reduced risk of bad investments Decisions based on facts, not on assumptions Requires orchestration of new expert skill sets Provides context, comparability and measurability	Critical for any M&A deal Risk of missing hidden deal-breakers

The new diligence

How do you know what's going to be a game-changer? Do you know which horse to bet on?

Technology is changing at the speed of thought. And since it is driving business on the information superhighway, investors want to be the first to spot the next big thing ahead. They are focused on smart tech such as IoT, automation, AI and digitalization. However, as co-travelers on the ever-changing territory of infonomics – monetizing information as well as the resulting intelligence – investors need to be able to see beyond the bend in the road. Especially when assessing the potential of a tech firm that has aroused their interest.

Here, business practices not tailored for smart tech tend to hit a brick wall. The "classical" due diligence approaches for Mergers & Acquisitions (M&A) alone are just not sufficient for a fair and efficient assessment.

Why?

For the simple reason that tech startups do not have classical assets and generally do not behave in familiar ways.

Tech is a shape-shifter that does not conform to traditional rules. It likes to spring a surprise. Tech startups – potential unicorns, after all – may not enter the profit zone for a long time. The winning bet is most often the idea, the code, the information assets, the proof of concepts or the future results expected of the company, rather than conventional balance sheet criteria.

No surprise, then, that "classical" methods, effective as they are, fail to convey the whole picture when assessing an M&A candidate from the tech field. Or even to leverage the surprise. Historically, top-notch consulting firms and lawyers are relied upon to check the health of a target's assets and its legal and financial build. But if a startup's true value lies in its intellectual property (IP), the scope of scrutiny needs to expand. IT infrastructure and security, for one, are then no longer one operational issue among others. They have taken center stage.

Consider a – fictitious – fintech startup with impressive prospects due to its uniquely effective user data management approach. Also imagine that you are assessing the viability of this target along the lines of traditional due diligence. Acquiring a startup with hardly any sales and highly valuable, yet equally vulnerable IP – what could possibly go wrong?

A lot, of course. That is why you have to check much more than its balance sheet, books and suchlike. In addition to traditional due diligence, it is essential to identify potential product risk, such as IP issues, and company-related risk, such as infrastructure weaknesses. To assess whether to ink a deal, a tech investor will therefore seek out ways to refresh the due diligence and expand it towards a "new diligence". In other words, schedule an upgrade!

And that is exactly what audius has been doing successfully for a number of years now.
Over a decade, audius has developed a toolkit for better informed decision-making, the **Loss Control Method**. Truly unique in its holistic orchestration of in-depth auditing across all operational channels, it delivers context and business intelligence in a reliable, outcome-oriented process. The approach achieves a healthy balance between adequate operational control and compliance with standards, laws and regulations. audius has contributed metrics to evaluate operational risks in M&A, helping you to make sense of the information technology, appraise security and risk, gauge trustworthiness, and put the intelligence gathered in a practical context. In recent years, more and more investors have employed our system to streamline M&A activities and get effective results faster.

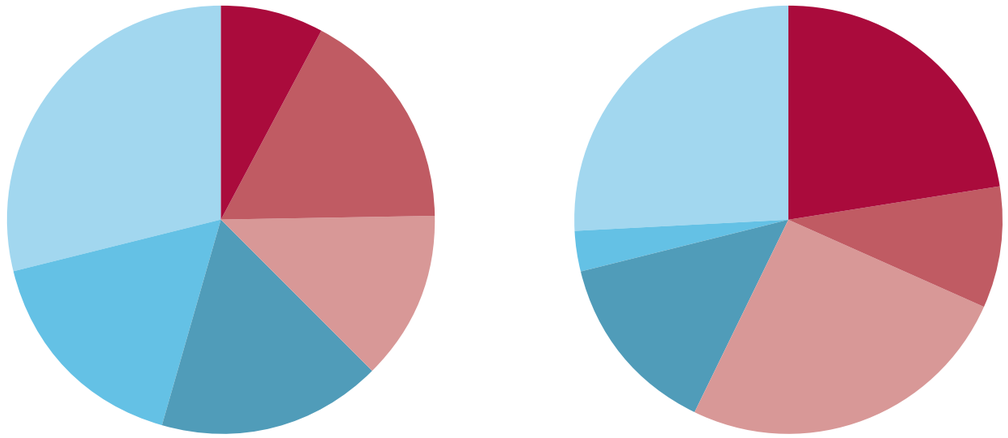
Our mission is **"From Risk to Business"**: a continuous process of assessing operational risk, implementing mitigations and treatments – and generating success. The result is three-pronged:

- **More realistic evaluation** obtained through transparency
- Investments to be made in future and associated **risks revealed early**
- **Impostors exposed promptly** as the gap between the marketing and the reality is laid bare

If you plan on going hunting, you need to acquaint yourself with the territory.

And as far as the M&A landscape is concerned, the territory has changed fundamentally in recent years. For instance, a noticeable shift has occurred in the motives of audius clients for using our operational due diligence approach. Statistics we extracted from over 200 security and audit projects for 35 of our clients show that operational due diligence projects to support M&A evaluation and decision-making have increased by 15% in the last three years.
The audius security and audit methods have always provided services across all industries, delivering a strategic approach to evaluating loss of control, security and operational risk. In the last 24 months, both small and medium enterprises (SME) and multi-national enterprises (MNE) have increasingly invested in digitalization by acquiring innovative companies and startups. Yet it is in the SME segment that the number of projects has grown most – from 7% to 31%.
M&A activity is gaining more and more important for smaller companies too. With our streamlined offerings, these businesses have access to highly efficient services that are not only fast but also affordable.

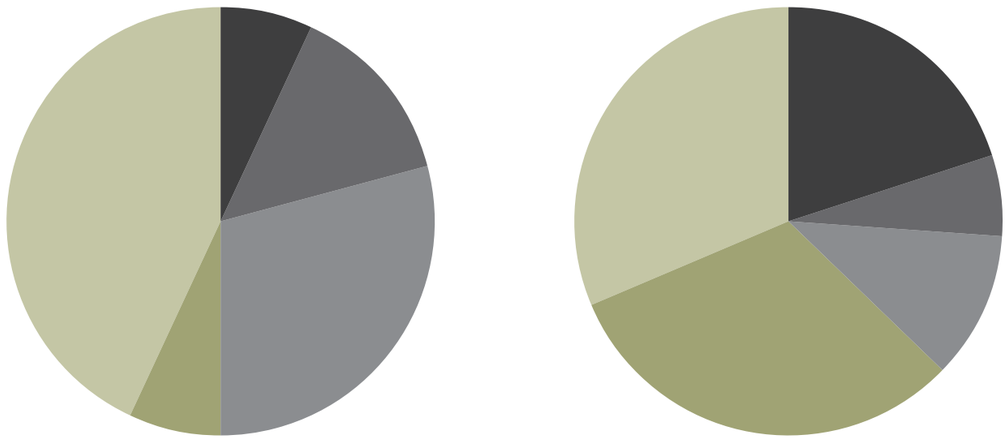
Motives before 2016 → Motives last 3 years



8% (De-) / Investment / M&A
17% Strategy Development
13% Indemnification Requirements / Compliance
17% Improve Organisation InfoSec
17% Improve Product Security
29% Improve Infrastructure Maturity

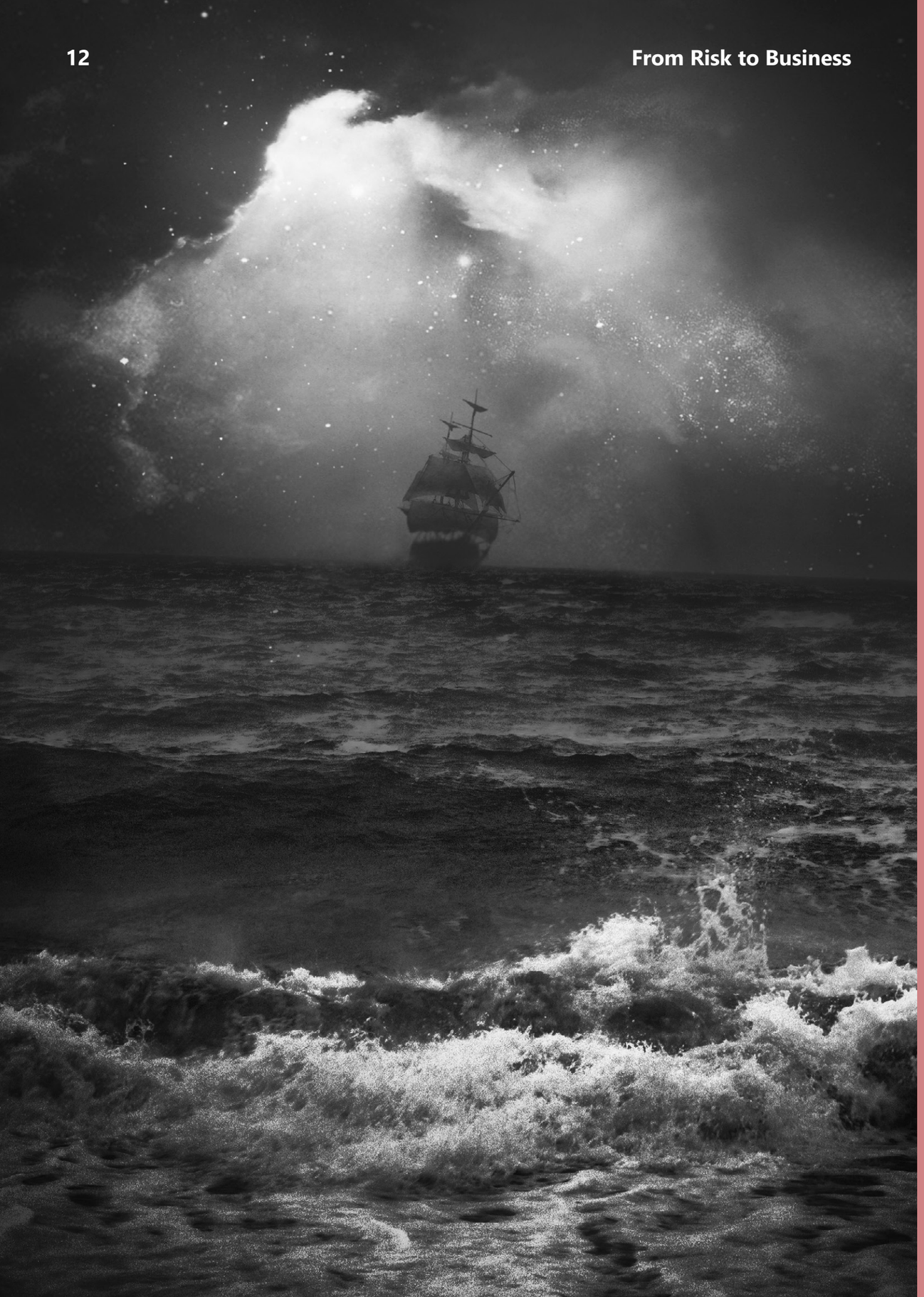
23% (De-) / Investment / M&A
9% Strategy Development
26% Indemnification Requirements / Compliance
14% Improve Organisation InfoSec
3% Improve Product Security
26% Improve Infrastructure Maturity

Industry Distribution before 2016 → Industry Distribution last 3 years



7% Healthcare
14% Finance
13% Public & Goverment
7% SME
43% MNE

20% Healthcare
6% Finance
11% Public & Goverment
31% SME
31% MNE



From Risk ...

Don’t believe, verify. And to verify, look beyond the apparent.
The due diligence audius performs to assess smart-tech candidates puts the firms, whether young or old, through deep technical checks to reveal their inner workings. This unearths any concealed risks facing the company right at the outset and predicts their practical consequences. We define risk by three elements: the threat, its impact and the probability of occurrence. The audius approach focuses on detecting unknown threats – and checking how likely known threats are to occur.

Such threats could be a **deal-breaker** if detected. And if undetected, they could cause **extreme financial injury**. The following real-life examples illustrate some such scenarios encountered by **audius** and extrapolate their respective damage potential.

Risks from Product Cluster

Threat

SPURIOUS PRODUCT

The idea, product or a number cited is not genuine; there is no proof the product works as claimed

Example: Features are touted but do not work for users

Maturity of product and user or product numbers lower than expected

Investors are oversold the merits

TECHNICAL VULNERABILITIES

Software or hardware open to system breach

Example: Backdoor in IoT device which could be exploited by an attacker

Noncompliance, leading to a tainted reputation

(Often this can be fixed with money)

BASIC SECURITY DESIGN FLAW

Example: Outdated or hazardous chipsets, like some that work with dangerous radio waves Easy accessibility, like reboot from a normal USB key

Cause for liability

Having to start from scratch

High financial damage

Irreparable, therefore a deal-breaker

ARCHITECTURE DESIGN FLAW

Example: Code or infrastructure cannot be scaled

Non-functional flaws in maintainability

Low scalability and usability

Business flops

TECH ABOUT TO GET OBSOLETE

Chipsets shipped, but not supported by vendor in near future

Ageing IoT hardware integrated with customers

A lot of avoidable legwork

Entire framework shatters

Hefty bill for repairs owing to heavy maintenance costs

INTELLECTUAL PROPERTY RIGHTS UNCLEAR

Example: It is ambiguous who owns the idea Wrongful use of open source code, or bad code Use of libraries that do not allow commercial use or proprietary development

Future obligations and liabilities

Unsolvable dependencies

Legal tangles and license dependencies

Can necessitate redevelopment

LACK OF SELF-AWARENESS

Example: The alleged USP is not so unique as the product developed "in a basement" already exists in a bigger and better form

Big investments needed to overtake established competition

Investor left playing catch-up

Likely Impact

Risks from Company Cluster

Threat

LOW "BUS FACTOR"

The 'nerd in your basement' is literally one of a kind and if they get run over by a bus, hypothetically speaking, it's game over

In more life-affirming words, there is no sharing of information among key team members

STAFF SHORTAGE

HR has low capacity

UNSECURE WORKSPACES, SHAKY INFRASTRUCTURE

Insufficient or absent security controls, e.g. in a shared workspace

Weak password for database access, credentials lying wide open

DUBIOUS DEVICE ORIGINS

The software is not company-owned, in which case it could be owned by just about anyone

GAPS IN PROCESS, POOR MANAGEMENT

Example: No security profiling for a feature

Missing change controls for hardware in transit

"GLOOMY" CLOUD ENVIRONMENT

Your cloud doesn't have the 'silver lining' of security, and invites attackers to "pwn" you, as the internet slang goes (i.e. to own you, to dominate you)

Project in limbo, if alive at all

Work underway at a snail's pace

You could lose control for good

No money for to make fresh hires → slow or no progress → dip in sales → even less money

Company assets left vulnerable

IP leaks before the ink is dry: Code being sold as IP ends up in a public repository

A Public Relations nightmare unfolds

Digital assets with high loss of control

Data theft

Waste of resources because of inefficiencies

Need for update in supply chain, change and security; then re-rollout

Hardware backdoors by a foreign entity

Digital assets with high loss of control

Loss of IP which is costly to fix

Data protection regulation (GDPR) breach and ensuing damages

Likely Impact

… to Business - The Method

Now to the heart of the matter.

How do we ferret out the threats menacing a company which a normal audit would have missed? In relatable terms, think of it as the M&A audit that you already know but under a well-calibrated magnifying glass with a new scope.

As it is, mergers and acquisitions are exacting, protracted processes. To add more complexity to this makes little sense. So audius has worked out a method which plumbs the depths without taxing the already arduous process more than necessary.
The **Loss Control Method** – our well-adjusted magnifying glass, so to speak – is sturdy. It has been well-tested and proven and sets us apart.

The method employed today by our Security & Audit Service in fact germinated in our engagement within an ecosystem of IT communities spanning the globe that work towards enhancing the world's experience of technology. As such, audius became the go-to player in the field – particularly for tricky penetration tests (which only insiders are privy to).

It was during our contributions, in the form of research and other support, to Fedora Project, Alpine Linux, ISECOM, home-assistant.io, expIIoT, nullcon, null-community and hardwear.io among others, that the **Loss Control Method** began taking shape.

Building our reputation with the Security & Audit Service over a decade, the **Loss Control Method** has equipped audius to deliver results quickly and with reasonable effort. On top of that, we have ensured that our operational due diligence talent is armed with a whole cluster of skills to contribute to M&A projects for investors worldwide. In fact, the efficient orchestration of expertise is one of our main competitive advantages.

Today we cover the whole plane of a tech check with a **quadruple assessment:**

Spectrum Channel – SpecOps
(Wireless)

Human Channel – HumOps
(Processes, Compliance)

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

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

The checks empower the interested parties to make decisions based on verifiable fact – and not just approximation, best practice assumptions or feeling – by supplying a trifecta of **context, comparability and measurability.**

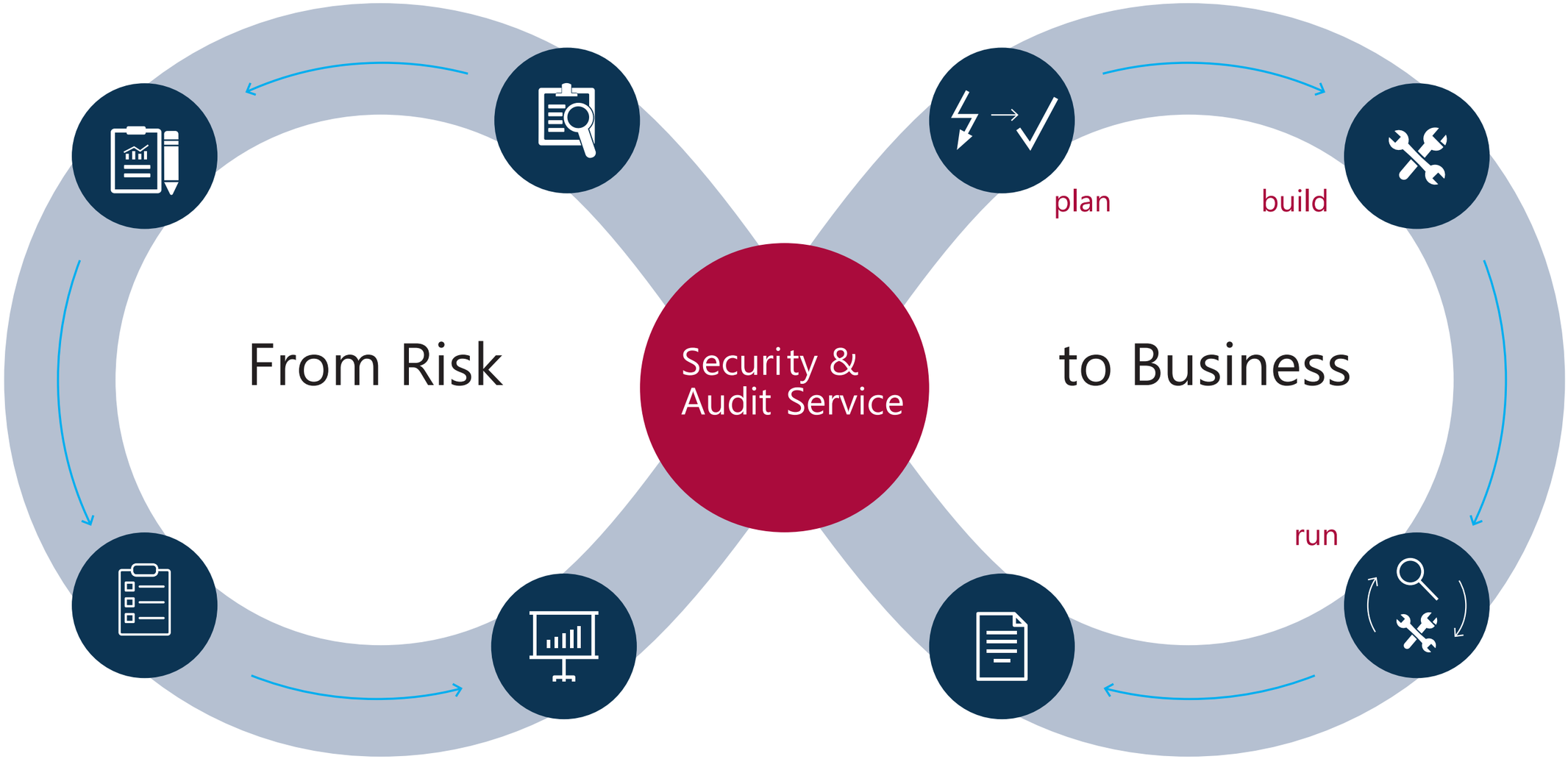
We learned quickly that even the most dazzling discovery – findings that blew our minds – was of little value without an appropriate context and the propensity to be measured or compared. And rather than restricting ourselves only to IT, we compiled penetration testing, infrastructure maturity assessments, compliance management, process management and risk management in an unparalleled approach. At the end of all this labor was born the Loss Control Method. It helped us remain true to our motto, **From Risk to Business**, and became the whole and soul of our mission. Though it was harder than we initially anticipated, we were finally able to get to the bottom of the question: "What does it mean for your business?"

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!

Conceptually, the Loss Control Method is based on an approach that evaluates an organization's "loss of control" for particular assessment properties or assessment channels.

It uses unbiased metrics and produces comparable results. This in turn enables the analyst to define the gap between the as-is and the "Ideal Loss Control". Only after you have identified a gap can you proceed to close it in a controlled manner. The method has been expanded and refined, so as to encompass a variety of functional and also non-functional requirements of operations; "functional" referring to the core functionality, "non-functional" to properties of operations as a whole. These non-functional requirements such as resilience, confidentiality or maintainability of course also matter a great deal to businesses. With this method, audius delivers insights, metrics and transparency regarding operational risk, security and readiness – abbreviated as OpRisk, OpSec and OpReadiness – for all assessment channels: efficiently, objectively and fast.

→ **OpRisk**
Operational Risk refers to building intelligence on how business continuity is established, and how a company or product is able to handle high loads quickly as well as cope with emergency situations like attacks and any disasters. In particular, non-functional requirements like availability, short-term scalability and resilience are analyzed, considered and measured.

→ **OpSec**
Operational Security concerns intelligence on access, treatment of secrets and information, and how these are secured. More specifically, the focus is on non-functional requirements like confidentiality and change control.

→ **OpReadiness**
Operational Readiness gathers intelligence on how the business operations are managed, documented and prepared for the future. In this domain, non-functional requirements like efficiency, maintainability and long-term scalability are of particular relevance.

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.

Data Protection
Holger Zürn
and Team
Processes and Management Systems
Juliane Scholz
and Team
Methods, Metrics and Intelligence
Steffen Lier
and Team
IoT, Cloud & Innovation
Stephan Traub
and Team
Standards & Compliance
Markus Biche
and Team
Security & Penetration Testing
Jens Mücke
and Team
Open Source & Open Standards, Code-Licensing
Jan Berens
and Team
Infrastructure
Michael Mederer
and Team
Physical Risk
Markus Biche
and Team

Why audius?

There are many answers to this question. The high caliber of our market-leading services results from decades of experience, state-of-the-art technologies, certified quality management and award-winning innovations. But in the end, it boils down to our ability to listen – "Erfolg durch Zuhören", as our motto has it. For us, focusing on our customers' actual business needs is the foundation of success – theirs and ours.

Our history as a business has been a continuous trajectory of rapid growth. Founded 1991 as an IT distributor with a workforce of four, audius has since evolved to a leading medium-sized German software and IT services provider with close to 500 employees, global operations and numerous subsidiaries. Our customer base now includes organizations from all industries and sectors – medium-sized companies, global corporations and public sector institutions.
What has not changed over the decades is our company-wide team spirit. We are still an owner operated business with lean structures and effective decision processes. This is why audius is able to provide bespoke solutions efficiently and quickly. As the saying goes, it's not the big that eat the small. It's the fast that eat the slow. The same values prompted us also to develop our operational due diligence services, a solution specifically tailored to mergers & acquisitions deals in the infonomics and startup space: We wanted to help dynamic businesses go the extra mile in their M&A due diligence. Technical expertise, total dedication to customer's needs, unique approach with proven track record – these typical audius traits characterize our operational due diligence services just as well as our company's numerous other offerings.

Our wide service range includes:

- **High quality IT services, consulting and cloud solutions**
- **CRM systems for customer service and sales**
- **Mobile enterprise application platform for all business sectors and areas**
- **Mobile data infrastructure**

audius
Mercedesstr. 31
71384 Weinstadt
www.audius.de

Contact:
Joerg Simon
Division Director Security & Audit Services
joerg.simon@audius.de
+49 7151 36900 337

audius