Special Edition
IT Summit

United Innovations

Survey of Tools for Intelligent Systems, Secure IT and Enterprise Innovation

Release 2025

www.united-innovations.eu

IT SUMMIT GERMANY

Join the IT Summit Germany 2025 on June 26th in Frankfurt, where industry leaders and innovators will explore the latest advancements in AI, software development, cybersecurity, and witness the exciting finals of the German Startup-Cup.

26/06/2025
9:00 AM

KFW
PALMENGARTENSTRASSE 5-9
60325 FRANKFURT AM MAIN

JOIN NOW

www.united-innovations.eu/it-summit-germany

EDITORIAL

Kathrin Scheld

Dear readers,

on June 26, 2025, the IT Summit at KfW in Frankfurt am Main will be a central event in the innovation landscape. With around 400 expected guests, the summit offers a rich and varied program featuring thought-provoking panel discussions, inspiring keynotes, interactive round tables, and the German Startup Cup. The event will also include a compact trade exhibition showcasing pioneering technologies and forward-looking academic approaches.

In this edition, you'll find a range of insightful articles on software development, cybersecurity, and artificial intelligence. Among the key questions we explore are:

- How can AI autonomously detect bugs?
- Why must DORA and NIS-2 be integrated into service management?
- Why is it time to rethink our understanding of cybersecurity?
- How can GenAI be successfully implemented across an organization?
- How can companies protect themselves against top Industry 4.0 and OT security risks?
- Why are AI risk management and testing tools gaining momentum?
- What does it take to master data quality?

In addition, we delve into topics such as the transformation from SAP ECC to S/4HANA, navigating the Digital Operational Resilience Act (DORA), and the role of synthetic test data in future-proofing IT systems.

Discover how low-code platforms can modernize legacy systems, streamline processes, and boost responsiveness to change—securing long-term competitiveness. Learn which methods and tools truly support data-driven decision-making as a key success factor for businesses.

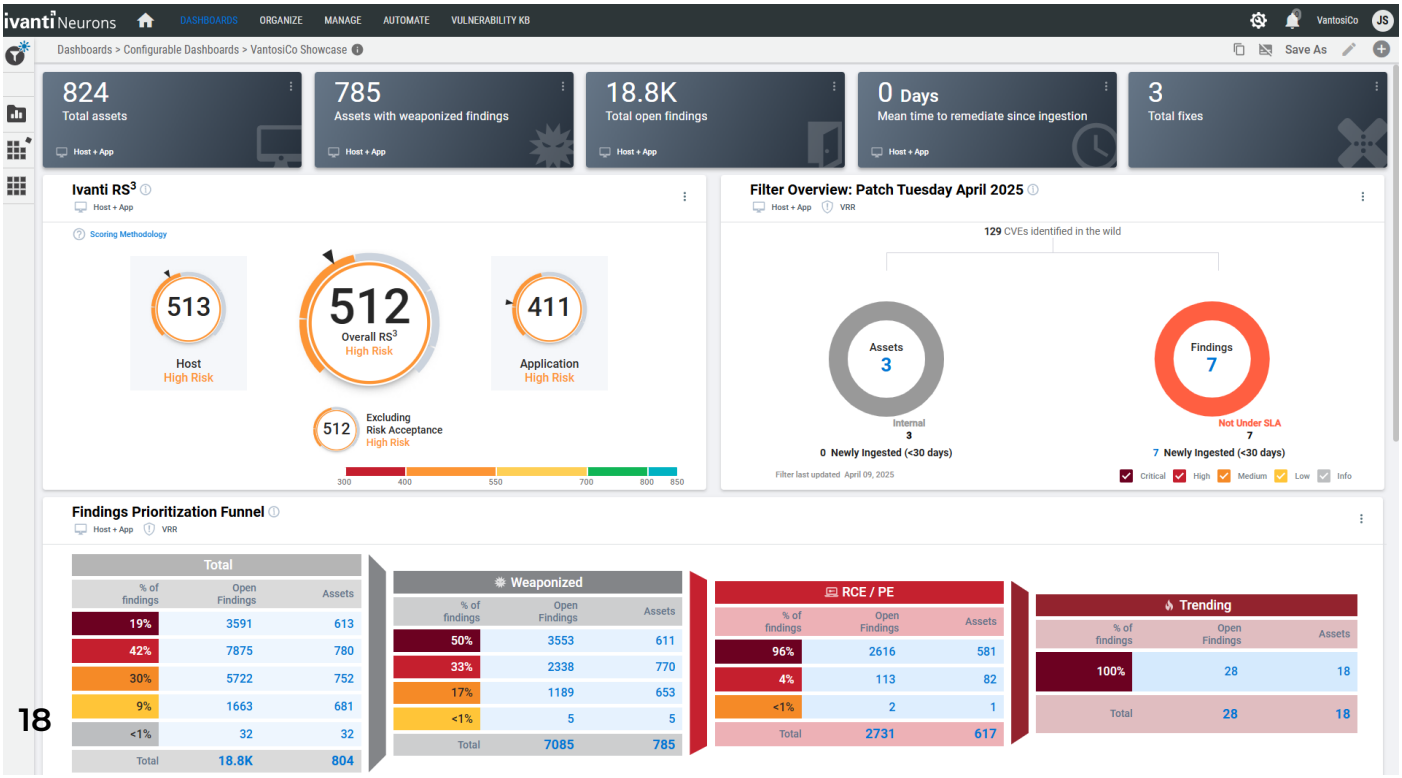
A special thank you goes out to all contributors, speakers, and participants who have made the IT Summit possible. Your expertise and dedication are what drive our community forward.

We hope this edition offers you fresh perspectives and inspiration.

Enjoy reading,

Kathrin Scheld

CMO
GFFT Security Lab GmbH



18

26

30

CONTENT

Content

UNITED INNOVATIONS

Cybersecurity

Strategic Perspectives & Partnerships

AI-Driven Security & Operational Protection

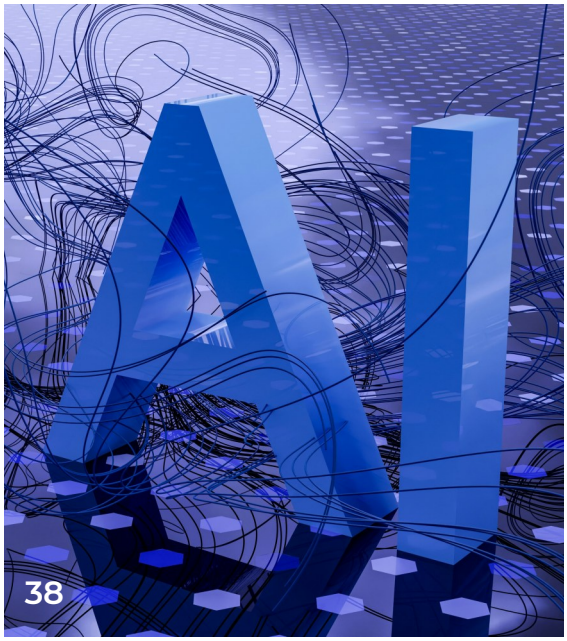
CONTENT

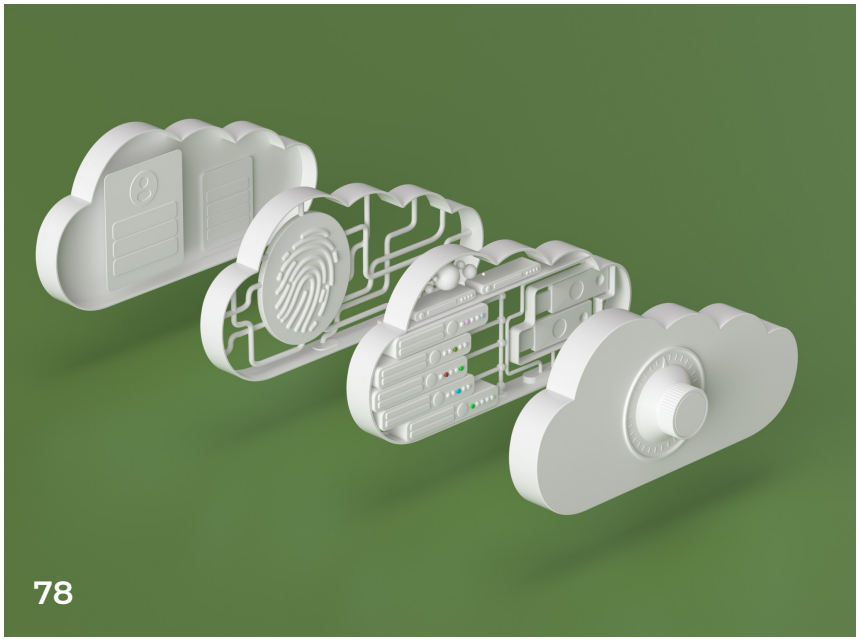
Software & AI

Strategy & Digital Transformation

Applications & Innovation

Risk & Quality Management





CALENDAR

17/09/2025 15:30-17:00	Software Insights: Guide and Collection of Methods for Implementing DORA in Software Testing (German) Info & Registration
18/07/2025 15:30-17:00	Security Insights: OT-Security (German) Info & Registration
23/09/2025 15:30-17:00	Software Insights: Digital euro: opportunities and challenges on the path from theory to practice (German) Info & Registration
24/09/2025 15:30-17:00	Software Insights: Target Pictures in Enterprise Architecture Management (German) Info & Registration
25/09/2025 15:30-17:00	Security Insights: Post-Quantum Cryptography (German) Info & Registration
02/10/2025 15:30-17:00	Drivers of Cybersecurity (German) Info & Registration

Take part in an event

If you are interested in participating in a workshop or event, you can either register directly via our event page or send us an email at info@united-innovations.eu. You will then receive the dial-in details.

All events and further information can also be found at www.united-innovations.eu/events

Discover Our YouTube Channel!

Did you know that our magazine has been on YouTube for quite some time? Visit our channel at the following link: GFFT YouTube Channel.
On our YouTube channel, we offer a wealth of valuable content:

- Startup Pitches: Discover emerging startups and their innovative ideas and products.
- Use Cases: Learn how creative solutions are implemented in practice and the value they provide.
- Panel Discussions: Follow engaging discussions with experts from various industries on current topics and trends.

Stay informed and get inspired. Subscribe to our channel to never miss new videos and always stay up to date.

United Innovations

Driving European Innovation Forward

United Innovations (UI) is a dynamic force reshaping Europe's innovation landscape. Our mission is to enhance efficiency in large corporations and promote the adoption of cutting-edge methods and technologies. UI focuses on increasing the success rate of new technologies in Europe, bolstering the continent's reputation as a leading innovation hub.

At UI, we emphasize collaboration through our innovation network, enhancing efficiency, quality, and reducing costs. Our partnerships expedite innovation cycles, facilitating the successful launch of new advancements.

Our innovation strategy revolves around identifying innovation needs, assessing current methods and technologies, and establishing effective innovation processes, including the development and implementation of new solutions.

United Innovations invites you to be part of this vibrant evolution in Europe's innovation sector. For more information, visit www.united-innovations.eu or follow UI on LinkedIn.

Contact

info@united-innovations.eu
+49 6101 95498-10

Our vision

Social Media

www.linkedin.com/company/gfft-ev/

www.youtube.com/GFFTeV

Imprint

GFFT Innovationsförderung GmbH
Dr. Gerd Große
Niddastraße 6
61118 Bad Vilbel

Web

www.united-innovations.eu

Print

Flyeralarm GmbH

IT Summit Germany 2025 – Focusing on Future Technologies

On June 26, 2025, United Innovations (UI) invites you to the IT Summit Germany at the KfW headquarters in Frankfurt am Main. As the initiator of this premier event, we are delighted to welcome around 400 experts from the fields of technology, cybersecurity, and innovation, with KfW as this year's host.

The IT Summit is the central meeting point for those interested in the latest developments in artificial intelligence, software development, and digital security. Featuring groundbreaking solutions and insightful discussions, the event provides key impulses for the future of these vital fields.

A major highlight of the summit is the **German Startup Cup**, where winners will be crowned in the categories of **Cybersecurity** and **Software & AI**. Finalists will present their innovative solutions to an expert jury and the audience, who will jointly determine the champions.

High-Level Talks and Discussions

The diverse program includes engaging presentations and panel discussions led by top leaders in the IT industry. The event will focus on strategic approaches that help companies leverage technological advancements to stay future-ready. Special attention will be given to the role of AI and the transformation of digital security in agile enterprises.

Experience Innovation and Connect

The IT Summit also features exhibition booths, where startups and technology providers will showcase their latest advancements. Take advantage of the entire day to network, gain valuable insights, and exchange ideas with some of the brightest minds in the industry.

Join Us!

Don’t miss the opportunity to stay at the forefront of technological innovation on June 26, 2025, at the IT Summit Germany in Frankfurt. Spaces are limited – secure your spot today and actively shape the future of IT!

Tickets: www.united-innovations.eu/tickets-it-summit-germany/

DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS

IT Summit Germany
Focus on Future Technologies

Join us on June 26, 2025, at the KfW in Frankfurt for a day of innovation. Explore advancements in AI, software development, and cybersecurity, connect with leaders, and shape the digital future.

Look forward to participants such as:

Tickets & Infos

Franz Ackermann
Manager | ICT Risk Management, **Deutsche Börse**

Carsten Frey
Direktor IT-Betriebsservices, **KfW**

Jochen Friedemann
CISO, **Talanx / HDI Group**

Nikolaus Hagl
Mitglied der Geschäftsleitung, **SAP Deutschland**

Benedikt Heintel
CISO, Director Proteciton & Resilience, **Viega**

Dr. Tobias Herwig
CTO, **Swiss Life**

Hermann Huber
CISO, **Hubert Burda Media**

Stephan Müller
Division Manager IT / CIO NORD/LB, **Norddeutsche Landesbank Girozentrale**

Danny Scheinhardt
Head of Cloud Governance and Processes, **Commerzbank**

...and many more!

Michael Schorpp
Global Regulatory Affairs, Boehringer **Ingelheim International**

Richard Socher
CEO **you.com**

Thomas Theisejans
Chief Expert IT Notfallmanage-ment, **Deutsche Bahn**

Heiko Weber
EMEA Head of Information Security and Data Protection, **Linde Material Handling**

United Innovations
GFFT
KfW

Reframe your readiness: Setting new standards for managed services

Why do companies need to rethink their understanding of cyber security and how do innovative approaches contribute to this?

An article by r-tec

Cyberattacks, growing threat complexity, and a shortage of skilled professionals are posing significant challenges for businesses in the field of IT security. r-tec IT Security GmbH from Wuppertal supports companies in meeting these challenges—with services, technologies, and a completely new understanding of cybersecurity.

Companies cannot completely prevent cyberattacks—but they can prepare effectively. That's why r-tec's approach is: Reframe your readiness. "We don't see cybersecurity as a fixed state or merely a protective shield," explains Managing Director Dr. Stefan Rummenhöller, "but as a continuous readiness to adapt to new threats and remain capable of acting—both technologically and organizationally."

Since many companies lack the resources to operate the necessary technologies internally and set up their own teams of experts, r-tec's Cyber Defense Center offers a comprehensive service to ensure cyber security readiness. It operates similarly to a trauma center: experts from various disciplines quickly come together to assess situations, analyze incidents and threats, and simultaneously respond with targeted actions. Thus, companies gain access to modern technologies and qualified specialists without having to build up capacities themselves.

Implementing Innovative Ideas Requires Innovative Solutions

An important part of preparing for cyberattacks is being able to detect them at an early stage and respond effectively. This is where r-tec sets new standards with its managed services: the Managed Detection and Response (MDR) service combines expert-driven attack detection and incident response, leveraging Exabeam's innovative New-Scale Security Operations Platform. The solution from the five-time Gartner Magic Quadrant leader is the first of its kind to offer full Open API compatibility, enabling seamless integration with existing security tools without vendor lock-in.

As Exabeam's largest MSSP partner, r-tec relies on the SIEM specialist's software for good reason: "Exabeam's Open API platform enables us to tailor our MDR service even more precisely to the requirements of our customers and their individual threat situation," explains Sebastian Bittig, Director of Cyber Defense at r-tec. "Thanks to intelligent automation, advanced algorithms, and optimized analysis, we can detect and respond to attacks faster than ever." To provide the optimal solution for each customer, r-tec also offers the MDR service with Microsoft Sentinel as an alternative.

Effective Preparation and Rapid, SLA-Controlled Incident Response

For specialized monitoring of endpoints, r-tec also offers a Managed Endpoint Detection and Response (EDR) service. The service focuses on potential gateways in computers, smartphones and other devices, enabling attempted attacks to be detected quickly. This is made possible by

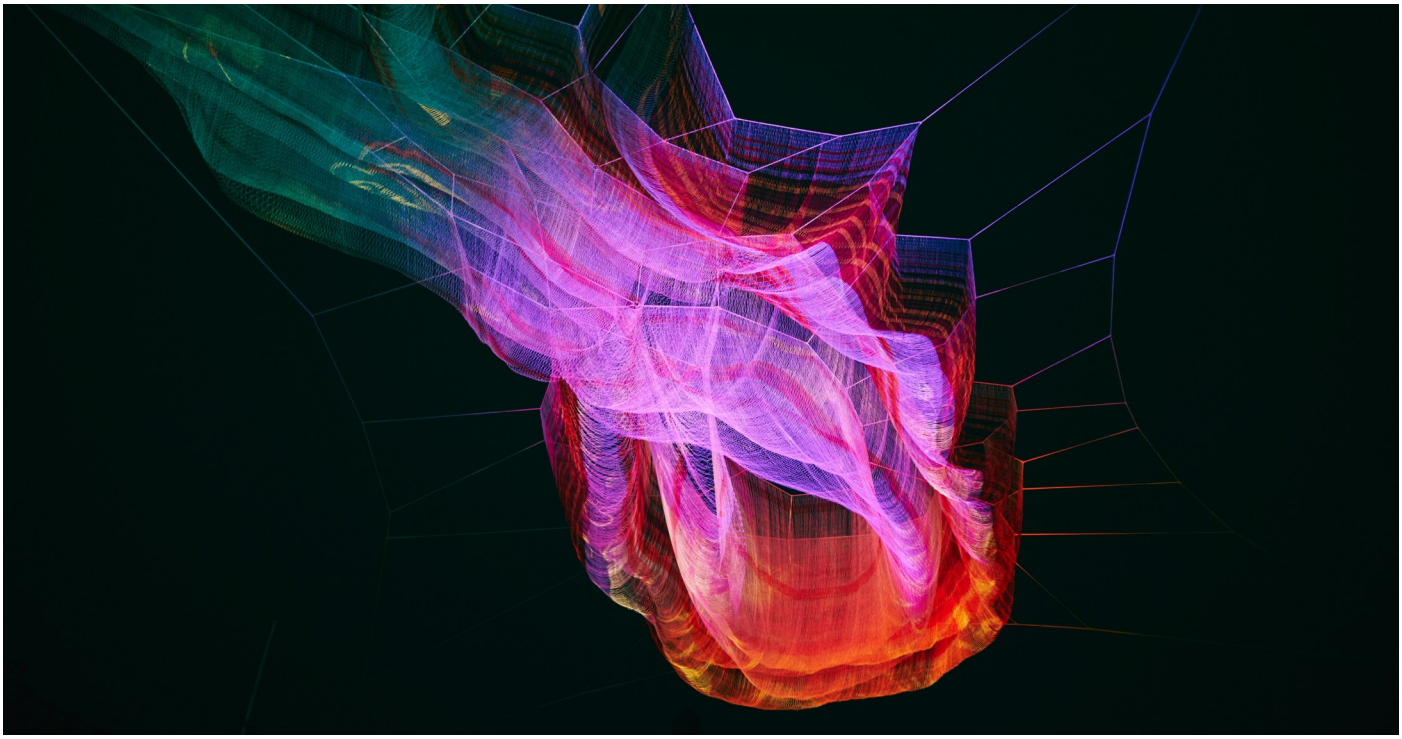


Image: r-tec IT Security GmbH

Falcon, CrowdStrike's market-leading next-generation SIEM solution – another leader in the Gartner Magic Quadrant. For Microsoft ecosystems, r-tec also offers the Managed EDR service with Microsoft Defender XDR. Both applications enable effective detection and defense against endpoint threats.

Speaking of defense: Whether an attack can be stopped or causes damage is also a question of speed and precision. The SLA-controlled processes of the r-tec incident response service therefore guarantee fast response times and targeted defense measures. Experts rapidly analyze threats, provide an initial assessment, and ensure threats are contained as swiftly as possible.

Cyber security is a question of future viability and capacity to act

Companies should abandon the idea that cyberattacks can be prevented or countered with protective software alone. It is crucial to expect attacks at any time and to be able to react to them. Under the guiding principle of "Reframe your readiness," r-tec is setting new standards in cybersecurity—defining security as a dynamic willingness to embrace change, innovation, and growth. "Our managed services combine state-of-the-art technology with leading expertise. We not only make companies more secure—we prepare them for future challenges," says Managing Director Marek Stiefenhofer. "Only those who anticipate threats can recognize them – and ensure that an attempted attack remains just an attempt."

Dr. Stefan Rummenhöller
Managing Director
r-tec IT Security GmbH

Sebastian Bitting
Director of Cyber Defense
r-tec IT Security GmbH

Marek Stiefenhofer
Managing Director
r-tec IT Security GmbH

Detailed information in the techL profile: r-tec

Why DORA and NIS-2 Must Be Integrated into Service Management

Regulatory requirements for IT security and resilience are increasing, with the Digital Operational Resilience Act (DORA) and NIS-2 Directive introducing stricter rules across the EU. These regulations overlap but focus on different aspects—DORA targets financial institutions, while NIS-2 applies to essential and important entities across various industries. Despite not yet being fully transposed into national law, organizations must act now to ensure compliance.

An article by Bert Kondruss, USU

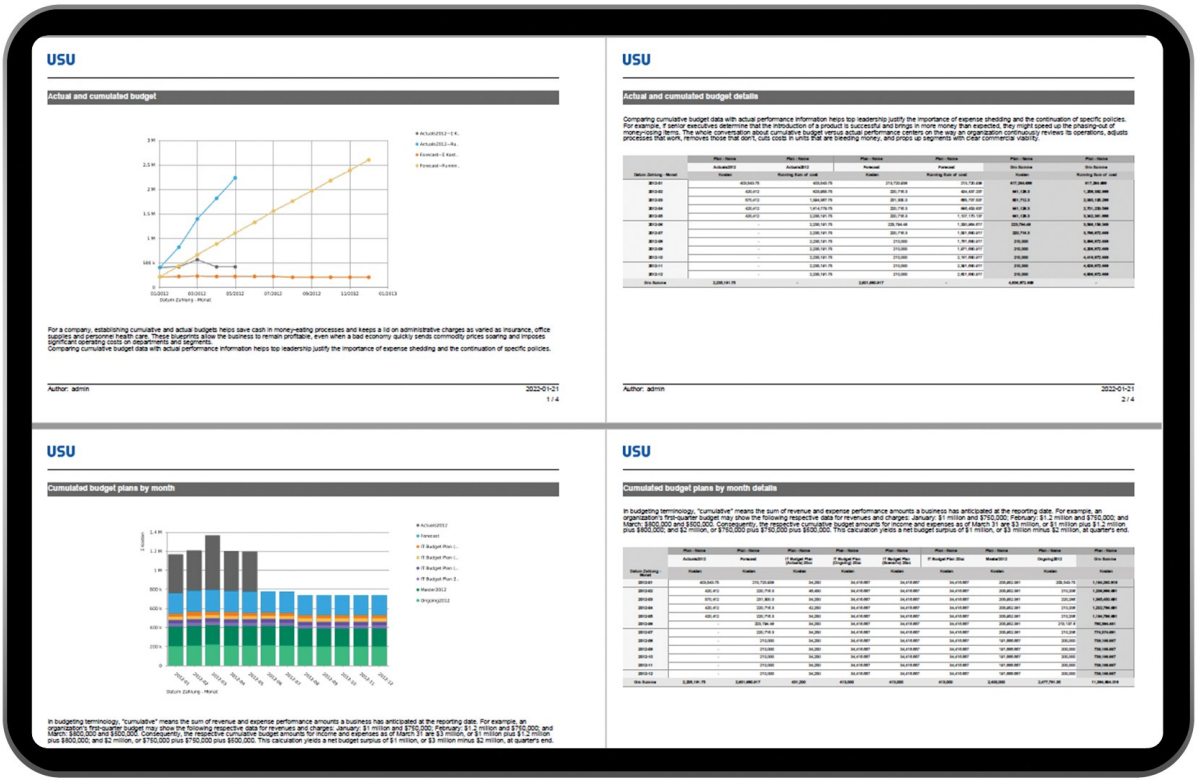


Image: USU GmbH

A major challenge in Governance, Risk, and Compliance (GRC) is managing complex data structures efficiently. Many companies still rely on Excel for GRC processes, but this approach struggles to handle the dynamic nature of IT landscapes. Instead, integrating IT Service Management (ITSM) and GRC creates a single source of truth - ensuring accurate, up-to-date information for CISOs, data protection officers, and auditors. This article explores why ITSM data is key to meeting DORA and NIS-2 requirements and how organizations can leverage USU's integrated approach to streamline compliance.

DORA and NIS-2: Overlapping Yet Distinct Regulations

DORA and NIS-2 share a common goal - strengthening cybersecurity and resilience - but they

apply to different sectors:

- **DORA** focuses on financial institutions, requiring them to ensure the resilience of their IT infrastructure, manage third-party risks, and establish incident response procedures.
- **NIS-2** applies to a broader range of industries, setting stricter cybersecurity obligations for essential and important entities such as energy, healthcare, and digital services.

Both regulations require organizations to manage risks, document security measures, and ensure timely incident response. This is where ITSM plays a crucial role.

ITSM as the Foundation for GRC

ITSM systems contain essential data for compliance, including:

- **Organizational structures** – Who is responsible for what?
- **Systems and assets** – What needs to be protected?
- **Services and dependencies** – How do disruptions impact the business?

By consolidating this information, ITSM provides a single source of truth for security, risk, and compliance teams. Rather than maintaining separate, static records, companies can build compliance directly on live ITSM data.

The Pitfalls of Using Excel for GRC

Many companies still manage GRC processes in Excel spreadsheets, which presents several issues:

- **Complexity** – IT environments are dynamic, making it hard to represent assets, dependencies, and risks in a simple table.
- **Data maintenance** – Ensuring up-to-date information requires constant manual effort.
- **Lack of cross-links** – Spreadsheets don't automatically reflect dependencies between IT assets, services, and risks.

A better approach is to integrate GRC into ITSM, using real-time data from Configuration Management Databases (CMDBs) and other ITSM modules.

USU GRC: Integrated Compliance Without Data Silos

USU GRC, a module of the USU ITSM Suite, offers a fully integrated approach to compliance. It connects ITSM data with:

- **Risk management** – Identifying and mitigating cybersecurity risks.
- **Audit management** – Ensuring regulatory compliance with documented processes.
- **Business continuity planning** – Maintaining operations during disruptions.
- **DORA information register** – Meeting specific documentation requirements.
- **Vulnerability management** – Keeping security threats under control.

By eliminating manual data transfers and avoiding media disruptions, USU GRC ensures accurate and efficient compliance reporting - directly from ITSM.

GRC: A Critical Topic for Business Leaders

IT is no longer a support function - it's the backbone of every business. If IT fails, the company stops operating. That's why GRC is not just an IT issue; it's a strategic priority for management. By leveraging ITSM data for compliance, companies can ensure resilience, improve efficiency, and stay ahead of evolving regulations.

Have you decided on your next steps? With DORA and NIS-2 enforcement approaching, we recommend integrating ITSM and GRC to simplify compliance and protect your future.

Bert Kondruss
Product Director
ITSM
USU GmbH

Detailed information in the techL profile: USU

Bringing Security to the Next Level: Integrating ITSM and RBVM

The IT and security landscape in organizations remains fragmented, at the expense of both efficiency and security. Ivanti explains how integrating a risk-based approach into ITSM is helping.

An article by Andreas Schmid, Ivanti

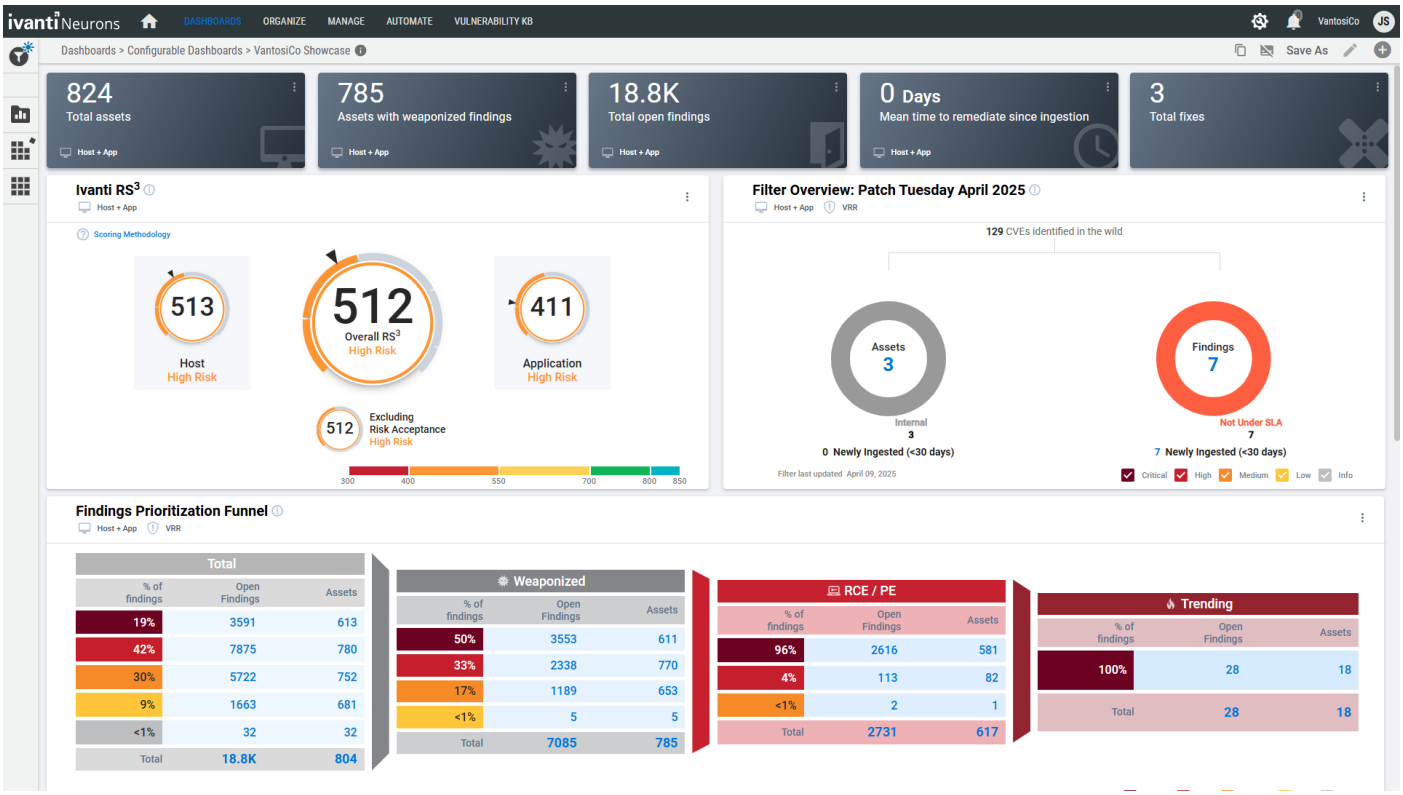


Image: Ivanti Germany GmbH

Traditional boundaries between IT and security teams are dissolving, but not without friction. Internal misalignments often lead to tension, delays, and vulnerabilities slipping through the cracks. The need for integration, visibility, and collaboration has never been more urgent.

The Challenge: Traditional IT and Security Silos

In many organizations, IT and security teams often work in silos, leading to conflicts and inefficiencies. Developers strive to release features rapidly, often without a deep understanding of security threats or best practices. Security teams are inundated with alerts and vulnerabilities, struggling to prioritize and communicate risks effectively.

This disconnect is exacerbated by disparate tools: developers rely on platforms like Jira or Azure DevOps, IT operations on ITSM systems, and security on vulnerability scanners. The result? Delayed responses, duplicated efforts, and a reactive rather than proactive approach to security—especially when vulnerabilities are discovered late in the release cycle.

Bridging the Gap: Integrating ITSM and RBVM

A unified, risk-based approach can help dismantle these silos. Integrating IT Service Management (ITSM) with Risk-Based Vulnerability Management (RBVM) enables early detection, prioritization, and resolution of security issues in alignment with business goals.

RBVM plays a pivotal role by pulling data from over 100 disparate sources (such as network scanners, endpoints, databases, IoT devices, manual research, pen testing teams) to provide a wide, unified view of cyber risk. By automating this process, RBVM eliminates the delays and human errors manual processes often introduce. This data is then enriched with essential context—such as severity, exploitability, and the criticality of the affected assets—so that vulnerabilities can be assessed more accurately. Rather than treating all issues equally, RBVM enables efficient and effective prioritization of the vulnerabilities and weaknesses, focusing remediation efforts to better protect against data breaches, ransomware, and other cyber threats. As a result, security teams can cut through the noise and focus their efforts on vulnerabilities and weaknesses that pose the highest risk, reducing the volume of issues they need to manage without compromising on protection.

On the other side, ITSM acts as the operational backbone that orchestrates and tracks remediation efforts. With a bidirectional integration, security can assign a prioritized list of vulnerabilities from RBVM directly into an ITSM ticket for fulfillment, while the IT team tracks and completes the remediation process. The system automatically creates and routes tickets—such as incidents or change requests—based on the nature of the vulnerability. These tickets are assigned to the appropriate teams, whether development, operations, or security, ensuring efficient and relevant handling. Ticket and status updates are seen in both teams' systems, allowing for full transparency throughout remediation.

Furthermore, the integration extends to development tools such as Jira and Azure DevOps, enabling seamless handoffs and real-time synchronization of ticket statuses and comments. Even source code management platforms like GitHub are tied into the process, providing traceability of code changes and supporting approval workflows before code commits are finalized.

Conclusion: The Future of Security Lies In Integration

Integrating ITSM with RBVM marks a pivotal shift in how organizations approach cybersecurity. By breaking down silos and automating workflows, companies can move from reactive defense to proactive resilience. Risk-based prioritization, shared visibility, and cross-functional collaboration ensure that security and IT becomes an enabler—not a barrier—to innovation.

As technologies evolve and threats become more complex, integrated, intelligent platforms will be essential. The journey toward a secure, agile enterprise begins with unifying people, processes, and tools.

Andreas Schmid
Director Solution Sales
Ivanti Germany GmbH

Detailed information in the techL profile:
Ivanti Germany GmbH

Crypto inventory – a must-have

In many companies, IT managers are currently faced with the task of preparing their cryptographic resources for post-quantum cryptography (PQC). This always starts with a crypto inventory. It can also be used effectively for optimisation and modernisation beyond PQC.

An article by Armin Simon, Thales

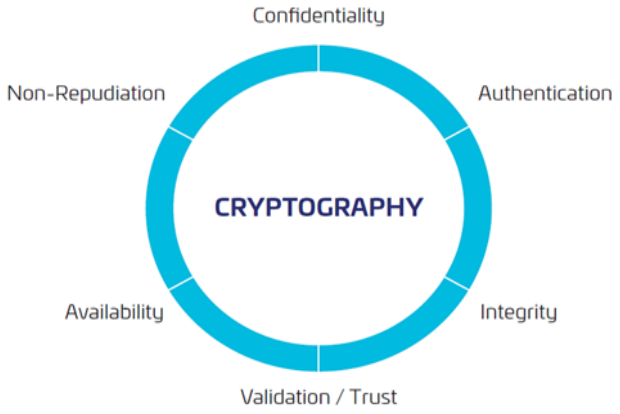


Figure 1: The new crytography framework for managing modern crypto inventories (from Thales, InfoSec Global, HSBC: Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow. 2025, page 8).

While preparing for the quantum age, many IT managers are currently faced with the task of converting their own cryptographic resources to quantum-resistant processes. To do this, they must first create a cryptographic inventory – a process that can also be used well beyond the quantum issue.

Cryptographic resources, such as keys, certificates, key memories, libraries, algorithms and cipher suites, play a decisive role in securing data communication. The quantum age is only a few years away and requires an adaptation of encryption methods, a migration towards quantum-resistant algorithms. To implement this, a comprehensive overview must first be created and all cryptographic resources must be recorded centrally – in a cryptographic inventory.

This process provides IT teams with an essential support for effective cryptographic migration into the quantum age. A cryptographic inventory is a dynamic, comprehensive and systematic listing of all current and evolving cryptographic instances within an organisation. It provides a standardised, detailed and comprehensive overview of where and how cryptographic objects are currently being used – in real time. As a result, it can also be used to optimise the management of cryptographic resources – both in terms of effectiveness and efficiency.

A cryptographic inventory helps:

- **to increase security:** Vulnerabilities such as unmanaged, expired or compromised certificates or outdated algorithms can be quickly identified and remedied.
- **to maintain compliance:** The comprehensive overview makes it easier to check whether all deployed cryptographic resources comply with current standards, enabling audits to be carried out quickly and easily.

- **to increase crypto agility:** If there are technical innovations that need to be implemented – as is now the case with post-quantum cryptography – an inventory helps IT teams to make the necessary adjustments seamlessly.
- **to optimise operational efficiency:** An inventory helps to simplify all recording and administration processes, which noticeably reduces the manual workload for IT teams.

For many IT teams, creating a comprehensive cryptographic inventory is a real challenge. Today's IT environments are highly dynamic and multi-layered. Legacy systems, cloud services, in-house applications and those from third-party providers are generally used in a colourful mix. IT teams need a structured plan, comprehensive expertise and special tools with which resources can be recognised and recorded automatically – ideally on an ongoing basis, so that the dynamics of the resources are reflected in the dynamics of the inventory in real time.

Despite all the complexity, the fulfilment of this task is essential. After all, cryptography forms the backbone of our trust in the digital world. And the framework conditions on which protective measures, regulations and expectations have been based up to now are just beginning to change – with significant effects on the management of cryptographic resources. The previous concept of the CIA triad, which was based on confidentiality, integrity and availability, is no longer sufficient on its own. It must be expanded to include three components: authentication, validation/trust and non-repudiation.

In the future, IT teams will have to evaluate all cryptographic objects regarding these six criteria as part of their cryptographic resource management. However, they will only be able to do this if they have previously compiled their cryptographic resources comprehensively and completely – within a modern, dynamic cryptographic inventory.

Armin Simon
Regional Director Germany
Data and Application Security
Thales

Detailed information in the techL profile:
Thales CPL

Partnership between TU Munich and Google in the field of cybersecurity and AI

An article by Georg Sigl, Technical University of Munich (TUM)

What are the patterns of cyberattacks on large language models (LLMs)? What role does data encryption play in ensuring online security, from web browsing to e-commerce transactions? Together with Google, the Technical University of Munich (TUM) wants to advance research in the field of cybersecurity. Last year, this partnership launched seven joint projects addressing critical challenges at the intersection of cybersecurity and artificial intelligence (AI). Two of these projects focusing on the intersection of hardware security and AI are highlighted below:

Cryptography is used in every electronic device today, e.g., to establish secure internet communication or to enable financial transactions. Protecting the cryptographic keys against unauthorized access is a major concern in today's electronic devices. Side-channel analysis allows extraction of secret keys used inside a silicon chip while it is executing cryptographic functions. Common side-channels are power consumption or electromagnetic radiation. Power consumption can be measured easily with an oscilloscope and a shunt resistor in the power supply. Such power measurements aggregate the complete power consumption of all active circuits of a chip and not only the interesting components executing the cryptographic function. Therefore, the signal to noise ratio is usually very low and the key extraction may be impossible.

To increase the measurement quality, we operate at TUM a security lab using an electromagnetic measurement probe, which allows local measurements. We move the probe with a diameter of 200µm at the tip above the chip surface and measure the electromagnetic radiation emitted through the switching transistors on the chip. On a training chip with a known key, we find those positions which give us the best measurement results. When attacking a chip with an unknown key, the challenge is to find the same position again with the highest precision.

This was the point where Google and TUM expertise came together. Google has excellent expertise in machine learning with neural networks and the necessary computing power to analyze millions of side-channel measurements to extract the secret keys with a neural network. This network has been trained on a training chip with known keys at positions which give the best measurement results. The challenge now is to find the same positions again on the attacked chip.

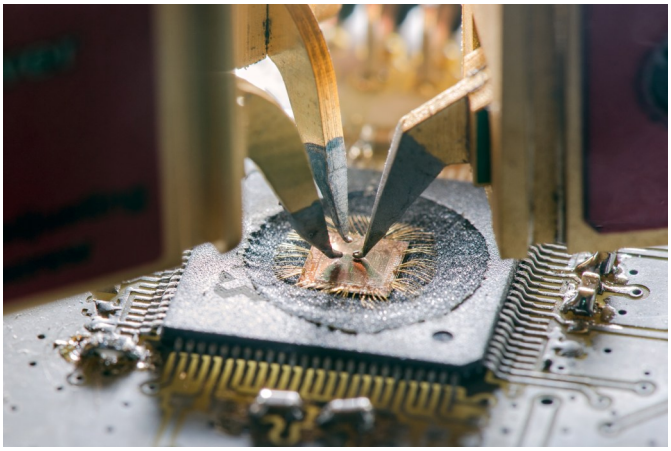


Image: Andreas Heddergott / TUM

Fig. 1: Picture of an opened chip with three probes placed above measuring in parallel.

At TUM we developed new techniques to identify the position of a probe by characterizing the electromagnetic field above a silicon chip like a three-dimensional landscape. Through comparison of this landscape between training and attack chip we can align the position of both chips. Google investigated an alternative method. They trained the neural network on the training chip with measurements from TUM including position variations. Finally, we compared both approaches. Currently it seems that position alignment before the attack with the neural network gives best results.

A second project focused on machine learning attacks on Post Quantum Cryptography (PQC). This is cryptography which will replace current asymmetric cryptography used, e.g., for signing software updates or financial transactions. Asymmetric cryptography can be broken by future quantum computers and must be replaced by new algorithms, i.e. PQC. These new algorithms are resistant to quantum computer attacks. TUM has very good experience implementing PQC algorithms in software and hardware. We implemented one of the first application specific integrated circuits (ASIC) including hardware accelerators for PQC [1]. Furthermore, our lab allows high quality power measurements of PQC implementations resulting unfortunately in almost terabytes of data.

The goal of Google in this project is to use their machine learning capabilities, which can handle such large amounts of data, to derive a secret key from these measurement data. In contrast TUM uses deep knowledge about the algorithms for alternative attacks. We are in the process to evaluate the results of both approaches. We know already that we can retrieve the keys of the currently standardized PQC algorithm Kyber, i.e. the new NIST standard ML-KEM. The TUM approach is even able to attack a protected implementation.

The two projects show the necessity to protect implementations of cryptographic algorithms against such sophisticated side-channel attacks. Highly skilled people and a broad interdisciplinary expertise are necessary to both attack the implementations and protect them against such attacks with proper countermeasures. These projects are therefore an ideal way to combine the strengths of TUM and Google and ensure a successful collaboration. We look forward to working together in these areas in the future.

More information on the other five projects [2]:

- *Secure compilation of high-performance concurrency models*: This project explores how to ensure that software customized for parallel computing architectures remains secure and free of vulnerabilities.
- *Large Language Models (LLMs) for the analysis of program code with regard to security vulnerabilities and data protection violations*: The focus of this research is on leveraging novel, LLM-based automated methods to identify privacy and security vulnerabilities in large codebases more efficiently and accurately.
- *Understanding attitudes and promoting acceptance of AI-assisted approaches to content moderation*: As LLMs are increasingly used to automate content moderation by identifying hate speech, sexism, and cyberbullying, this

study investigates their effectiveness and how they are perceived by human users.

- *Data protection risks of general AI systems: Stakeholder perspectives in Europe:* This project analyzes the potential data protection risks posed by general-purpose AI (GPAI) systems such as LLMs and examines how various stakeholders across Europe assess these challenges.
- *Understanding attacks on language models:* This project investigates how attacks on LLMs work, including malicious requests designed to extract private user data. It aims to understand what triggers such vulnerabilities in language models and how they can be effectively prevented.

References:

[1] https://www.tum.de/en/news-and-events/all-news/press-releases/details/translate-to-en-ein-post-quanten-chip-mit-hardware-trojanern

[2] https://www.tum.de/en/news-and-events/all-news/press-releases/details/tum-and-google-strengthen-cooperation

Prof. Dr. Georg Sigl
Professorship for Security in Information Technology
Technical University of Munich

Image: Astrid Eckert / TUM

Save the Date

SECURITY SUMMIT

Join us on March 17, 2026, at Vodafone in Düsseldorf for the Security Summit 2026, where industry leaders, researchers, and startups will come together to explore the future of cybersecurity, IT infrastructure, and digital resilience. Experience cutting-edge insights, breakthrough technologies – and the thrilling finals of the German Startup-Cup for IT Security.

17/03/2026

Secure Use of AI in Highly Regulated Industries

Artificial Intelligence (AI) is increasingly finding its way into businesses across all sectors - and for good reason. The technology offers immense opportunities. However, it also comes with significant risks, especially when dealing with sensitive data.

An article by Dr. Sebastian Eder, idgard

Image: Shutterstock / Gorodenkoff, licensed to idgard

AI opens up a wide range of possibilities across various application areas. In particular, Large Language Models (LLMs) offer substantial value to companies. These models are designed to process and generate natural language. Built on neural networks, they are trained on massive volumes of textual data. Well-known examples include OpenAI's "GPT" models, Mistral AI's "Mistral", and Meta's "LLaMA".

From automating complex tasks like data analysis and process optimization, to identifying specific data patterns or accelerating market assessments - LLMs bring considerable potential.

Nevertheless, their use also involves a number of critical risks, especially when handling sensitive data:

- Unauthorized access to training data or models
- Targeted manipulation of the model
- Data leakage during model execution
- Operational and maintenance complexity

As a result, traditional cloud and on-premises approaches often reach their performance limits when it comes to securely running AI applications.

Confidential Computing Enables Digital Sovereignty

Secure data processing in a sovereign cloud is made possible by Confidential Computing. This technological approach ensures that data remains protected during processing within so-called Trusted Execution Environments (TEEs). These environments prevent unauthorized access or manipulation, even if an attacker has physical access to the hardware.

One practical implementation is the Sealed Cloud technology. In this setup, data is processed within high-security server enclaves that are completely isolated from the rest of the system. This exceptional level of security not only ensures the reliable protection of confidential information during digital collaboration, but also enables the secure and sovereign operation of services such as collaboration tools - or even more complex applications like AI models—in the cloud.

How AI Moves into the Sovereign Cloud

To securely use LLMs in a sovereign cloud, the first step is to establish the appropriate hardware. This involves setting up a dedicated AI cluster on which open-source LLMs such as LLaMA or Mistral can be deployed. Once installed, the models are trained within the secure environment of the sovereign cloud and fine-tuned to meet specific user requirements.

It is essential that the entire process - from managing the training data, to training the models, to using them in production - takes place entirely within the sovereign cloud. This ensures full protection against data leakage and manipulation, and guarantees that user prompts - the input given to the AI - remain inside the secure environment. This approach enables sensitive data to be analyzed by AI, with results returned to the user without the service provider or any unauthorized third parties gaining access to either the data or the results.

In the future, it is conceivable to expand the AI cluster and offer it as a Platform-as-a-Service (PaaS). This would allow companies to develop and run their own AI applications in a highly secure environment - ensuring data integrity and full control over training data, models, and queries at all times.

Conclusion: AI Security in the Sovereign Cloud

Running LLMs within sovereign cloud services such as idgard, which leverage advanced security concepts like Confidential Computing, significantly reduces potential attack surfaces in AI deployment. Unauthorized access to training data, models, and prompts is prevented, and the risk of manipulation is greatly minimized. The high security level of Sealed Cloud technology enables companies to operate and further develop LLMs and other AI applications - without compromising on security or operational complexity.

Dr. Sebastian Eder
Chief Technology Officer (CTO)
idgard GmbH

Detailed information in the techL profile: idgard GmbH

How to Autonomously Find Bugs with AI

AI Agents not only simplify and accelerate software development but also enable autonomous security testing. Let's explore how Code Intelligence's AI Test Agent discovered the world's first vulnerability without human interaction — and continues to uncover more in open-source projects.

An article by Natalia Kazankova, Code Intelligence

Image: Code Intelligence GmbH

Even though companies rely on static analysis and penetration testing to secure their code, many vulnerabilities still make it into production. White-box fuzz testing has proven to be highly effective in detecting edge cases and security flaws early in the development process.

Now, with AI automation, white-box fuzzing can autonomously find bugs with a single command. This is how CI Fuzz by Code Intelligence has uncovered real-world vulnerabilities in widely used open-source software. Let's explore how it works and how you can apply it to test your software.

What is Fuzz Testing

Fuzz testing (or fuzzing) automatically provides random, unexpected, or invalid inputs into a program to uncover vulnerabilities or bugs.

There are two main types of fuzz testing:

- **Black-box fuzzing:** Operates without any knowledge of the internal code structure.
- **White-box fuzzing:** Leverages internal knowledge (e.g., source code or binary) to generate test inputs that maximize code coverage. This approach finds significantly more bugs than black-box fuzzing.

Learn more about the differences between the two approaches in this free Fuzz Testing Solutions Comparison guide.

Why Doesn't Every Company Use Fuzzing?

White-box fuzz testing is proven to be one of the most effective ways to find critical bugs and vulnerabilities. Tech giants like Google and Microsoft uncover thousands of security issues using this method. So why isn't it widely adopted?

The main barrier is the manual effort and time required to set up and maintain fuzz tests. You first need to identify what you should test, then implement corresponding fuzz tests, run them, and address the identified bugs.

However, with the rapid advancement in Large Language Models (LLMs), much of this process can now be automated.

From Start to Findings With One Command

Now, all manual steps can be done autonomously

by Spark, the first AI Test Agent that identifies bugs and vulnerabilities in unknown code without human interaction.

It's the first AI agent to find a real-world vulnerability by automatically generating and running a test for a widely used open-source software (wolfSSL).

With Spark, white-box fuzzing is now as simple as:

1. Setting up a testing goal (how much code coverage you want to achieve).
2. Launching Spark.
3. Reviewing discovered vulnerabilities.

When you launch **Spark**, it operates as follows under the hood:

1. Analyzes your codebase and **identifies the most important functions** and APIs to fuzz. Each fuzzing entry point is scored based on its expected impact using four key metrics.
2. **Generates fuzz tests** (harnesses) for each function by leveraging static code analysis to extract the correct context needed to test the target function and large language models (LLMs) to create and optimize the fuzz test.
3. **Runs and validates the generated tests** to ensure they can be built and run correctly and achieve high code coverage.
4. **Flags findings**, providing details such as the exact lines of code where issues occur, stack traces, and triggering inputs to assist in root cause analysis.

How AI Test Agent Uncovers Real-World Vulnerabilities

CI Fuzz, with its AI Test Agent, continues to find new in open-source projects, even those that have been fuzzed by other tools for years.

One of the uncovered and fixed vulnerabilities was in wolfSSL, an open-source cryptography library widely used in developing embedded devices and IoT systems.

The vulnerability was a heap-based use-after-free. The only human involvement in finding it was launching the spark command; analyzing the code, generating a relevant test case, and running it was done autonomously.

How to Start Using AI-Automated Fuzzing

If you're looking to strengthen software security with minimal manual effort, book a free call with our experts for a tailored demo of CI Fuzz and its AI Test Agent.

To start using AI Test Agent, you'll need to:

1. Install CI Fuzz.
2. Ensure access to LLMs.

During the call, Code Intelligence's experts will guide you through the setup process, share industry best practices, and provide insights on pricing options.

Natalia Kazankova
Principal Product Marketing Manager
Code Intelligence GmbH

Detailed information in the techL profile:
Code Intelligence

Revolutionizing Cyber Defense with AI-Driven Threat Detection

An article by Gregor Keller, Zscaler

Cyberthreats have evolved at an unprecedented pace, growing in both complexity and scale. In today's digital landscape real-time threat detection is no longer a luxury—it's a necessity. This is where automated processes supported by artificial intelligence (AI)-powered threat detection provides a transformative approach to cybersecurity that enables organizations to stay ahead of attackers. By leveraging AI, security teams can detect anomalies, automate response mechanisms, and enhance threat detection across vast amounts of data.

Traditional defenses, which rely on static rules and signature-based methods, struggle to keep up with ever-changing attack vectors and cybercriminals have outpaced conventional security measures by exploiting their gaps. Phishing attacks are using GenAI to create more realistic, personalized lures that can easily evade traditional filters and perimeter-based security that assumes internal trust fails to monitor lateral movement or detect threats once an attack gains access.

Core AI Technologies Powering Threat Detection

AI-powered security solutions rely on a suite of advanced technologies to identify and mitigate risks effectively. Machine learning (ML) can be used to detecting anomalies automatically by analyzing vast amounts of data to uncover hidden patterns. New techniques like Natural Language Processing (NLP) supports the examination of phishing emails and threat intelligence sources in real time. More importantly, deep learning can assist in profiling malware behavior to recognize subtle indicators of compromise and Adaptive AI is continuously learning from new attack tactics and adjusting defenses without manual updates. These technologies are enabling organizations to detect threats in real time and respond with unprecedented speed.

AI excels in processing massive data streams and identifying threats faster than any human analyst could with preemptive detection and response. By rapidly detecting anomalies, AI enhances threat detection across networks, reducing response times and mitigating attacks before they cause significant damage. Some of AI's most powerful real-world applications include:

- Identifying zero day exploits through behavioral analytics
- Preventing advanced persistent threats (APTs) before they infiltrate systems
- Stopping lateral movement within enterprise networks by dynamically segmenting users and devices

AI for Phishing and Social Engineering Detection

Phishing is becoming more targeted, with threat actors exploiting human voice, video and even using human psychology to craft personalized emails that appear legitimate to steal credentials or deploy malware. AI models combat phishing by analyzing email structures, language nuances, voice, video and embedded links. NLP-powered

Image: GettyImages-956550414 – royalty-free image licensed to Zscaler Germany GmbH

AI reduces false positives, ensuring security teams respond to genuine threats rather than chasing down benign alerts. By automating response mechanisms, AI threat prevention minimizes the damage caused by phishing campaigns.

Supporting Zero Trust Security with AI

A zero trust architecture (ZTA) is built on the principle that no entity—inside or outside the network—should be inherently trusted. AI plays a crucial role in enforcing this model by continuously verifying users and devices based on real-time behavioral analysis, blocking unauthorized access and lateral movement and dynamically adjusting access controls based on evolving risk scores. By integrating AI with zero trust organizations can analyze user behavior, identify anomalies, and enhance real-time security decisions to ensure secure, dynamic access to applications.

Cybersecurity is no longer just about defending against known threats—it's about proactively stopping emerging attacks before they strike. With AI-driven security and a zero trust approach, organizations can move beyond outdated, reactive defenses and embrace a dynamic, intelligent security posture. The Zscaler Zero Trust Exchange provides a comprehensive solution to modern cyberthreats. By integrating AI-powered threat protection, full TLS/SSL inspection at scale, and zero trust segmentation, this security platform minimizes attack surfaces, prevents compromises, and eliminates lateral movement. Whether securing AI-powered applications, detecting zero day threats, or protecting against data loss, Zscaler enables enterprises to operate with confidence in an increasingly complex threat landscape.

Gregor Keller
Senior Director Solution Consulting
Zscaler Germany GmbH

Industry 4.0 and OT security: How to protect your company from top risks

Cyberattacks aren't just happening more often, they are becoming technically more sophisticated. Production companies must understand their specific threat landscape to effectively protect their connected production infrastructure.

An article by Mareike Redder, TRIOVEGA

Image: TRIOVEGA GmbH

Insider threats, remote access, supply chain, and outdated machine control systems— manufacturing companies that digitalize their production must address multiple risk factors to minimize potential attack vectors for cybercriminals.

While short update cycles and modern encryption processes are common in IT today, OT machines and systems are often connected to the network for decades and are rarely updated. This challenge requires a targeted approach to effectively mitigate risks, which we will outline in the final section of this report. First, let's take a closer look at the most common threats to industrial companies.

1. Insider threats

When a company's employees - or external partners with access to parts of the organization - cause damage, this is known as an insider threat. These include both malicious and unintentional actions by the insider. A frequent entry point for malware remains phishing links in emails, which are inadvertently opened by a user.

2. Insecure remote access tools

Software tools for remote maintenance often use open network ports for communication - an

additional attack vector for cybercriminals.

In conventional network segmentation, this issue becomes apparent when hackers gain access to the network via open ports that are often not closed after use.

Attackers can then manipulate the production parameters directly or use the open door to explore the corporate network and gain access to other devices and endpoints. This is a common cyberattack scenario on industrial companies - malware sneaks in via a vulnerability in the production, and spreads throughout the IT systems.

3. Supply chain attacks

The introduction of the NIS 2 Directive in the EU wasn't the first time supply chains became a focus of cybersecurity efforts. Increasingly complex supplier networks and production lines, with numerous software and hardware components from different manufacturers, result in increased cyber risks.

Attackers can infiltrate the supply chain at various points, place manipulated equipment in deliveries, or install malware.

4. Outdated machine controls

Many machine control systems such as Programmable Logic Controllers (PLC), Computerized Numerical Control (CNC) machines, and Human Machine Interfaces (HMI) were developed in the 1980s and 1990s and are operated on Microsoft DOS (MS-DOS).

As machine manufacturers rarely provide updates, and in some cases, no longer even exist, companies often have no choice other than to continue running these machines on MS-DOS - an operating system that lacks integrated user or rights management and offers only limited encryption options via third-party encryption tools. As MS-DOS has not been updated for a long time, all known vulnerabilities remain open, and attackers can exploit the outdated SMBv1 network protocol, Telnet, or FTP, as attack vectors.

Even Windows XP, which was released long after MS-DOS, uses the insecure SMBv1 protocol, making systems vulnerable to attack if insecure services need to be provided to production environments by IT.

Shield production, but enable communication

The most recommended strategy to contain potential attacks is the complete separation of IT and OT networks.

With edge.SHIELDOR, TRIOVEGA developed a production security solution that decouples outdated OT systems - similar to the Air Gap Principle - while allowing regulated and controlled use of vulnerable protocols. This solution enables the connection to the company network.

Files transferred from the IT network using the secure SMBv3 protocol can be converted into SMBv1, still used by legacy machines, and synchronized with the OT network directory. The same can be done in reverse. The files to be transferred are continuously checked for malware signatures, and any threats are isolated, which enables communication with the system while reducing security risks.

By integrating edge.SHIELDOR into a central Active Directory, we also ensure that only authenticated users are able to access the connected services.

In summary, the complete separation of IT and OT networks, file conversion, and integration into user management help to effectively reduce attack vectors in production environments and provide additional protection for vulnerable production infrastructure.

Mareike Redder
Product Manager
TRIOVEGA GmbH

Detailed information in the techL profile:
TRIOVEGA

The Problem with Remote Access Tool Sprawl

An article by Thorsten Eckert, Claroty

Image: Claroty Ltd.

Insecure remote connections are becoming a favorite entry point for threat actors to use for an initial foothold on IT networks, as well as internet-facing operational technology (OT) assets such as industrial control systems (ICS). These exposures clearly pose a significant threat to companies, and are being compounded by excessive demands for remote access from not only employees, but also third parties such as vendors, suppliers, and technology partners.

Claroty, the cyber-physical systems (CPS) protection company, released new research from Team82 on remote access tool sprawl and the risk exposures it introduces to operational technology (OT) environments. Data from more than 50,000 remote-access-enabled devices showed that the volume of remote access tools deployed is excessive, with 55% of organizations having four or more and 33% having six or more.

Team82's research also found that a staggering 79% of organizations have more than two non-enterprise-grade tools installed on OT network devices. These tools lack basic privileged access management capabilities such as session recording, auditing, role-based access controls, and even basic security features such as multi-factor authentication (MFA). The consequence of utilizing these types of tools is increased, high-risk exposures and additional operational costs from managing a multitude of solutions.

Since the onset of the pandemic, organizations have been increasingly turning to remote access

solutions to more efficiently manage their employees and third-party vendors, but while remote access is a necessity of this new reality, it has simultaneously created a security and operational dilemma. While it makes sense for an organization to have remote access tools for IT services and for OT remote access, it does not justify the tool sprawl inside the sensitive OT network that we have identified in our study, which leads to increased risk and operational complexity."

While many of the remote access solutions found in OT networks may be used for IT-specific purposes, their existence within industrial environments can potentially create critical exposure and compounding security concerns that include:

Lack of visibility: In cases where third-party vendors connect to the OT environment using their own remote access solutions, OT network administrators and security personnel who are not centrally managing these solutions have little to no visibility into the associated activity

Increased attack surface: More external connections into the network via remote access tools mean more potential attack vectors through which substandard security practices or leaked credentials can be used to penetrate the network.

Complex identity management: Multiple remote access solutions require a more concentrated effort to create consistent administration and governance policies surrounding who has access to the network, to what, and for how long. This increased complexity can create blind spots in access rights management.

According to Gartner®, security and risk management (SRM) leaders should, "perform a full inventory of all remote connections across the entire organization, as shadow remote access likely exists throughout operational networks, particularly at field sites," and "remove older remote access solutions when deploying newer CPS secure remote access solutions. Organizations commonly deploy new solutions without focusing on what is left behind, and with the number of exploited VPN vulnerabilities growing, this could be a significant blind spot."1

Claroty's xDome Secure Access provides organizations with built-for-OT remote operations capabilities and OT-aware security architecture, delivering comprehensive visibility into both OT devices and the users connecting to them. The solution can now be deployed either on-premise or in the cloud, enabling organizations to optimize remote access management and reduce their total cost of ownership. Recognizing that no two CPS environments are identical, xDome Secure Access provides flexible, operations-specific remote access regardless of an organization's geographic spread, network architecture, or cloud maturity, all while enabling regulatory compliance with frameworks such as NIST and NIS2.

1 Gartner, Innovation Insight: CPS Secure Remote Access Solutions, Katell Thielemann, Abhyuday Data, Wam Voster, 18 April 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Thorsten Eckert
Regional Vice President
Claroty Ltd.

Information as a Key Success Factor in Enterprises

Data is one of the most valuable resources in modern enterprises, driving innovation, growth, and informed decision-making. However, many organizations struggle to harness its full potential due to various challenges. This article explores the current state of data usage, its evolution, and a vision for information-driven businesses.

An article by Tim Biedenkapp, adorsys

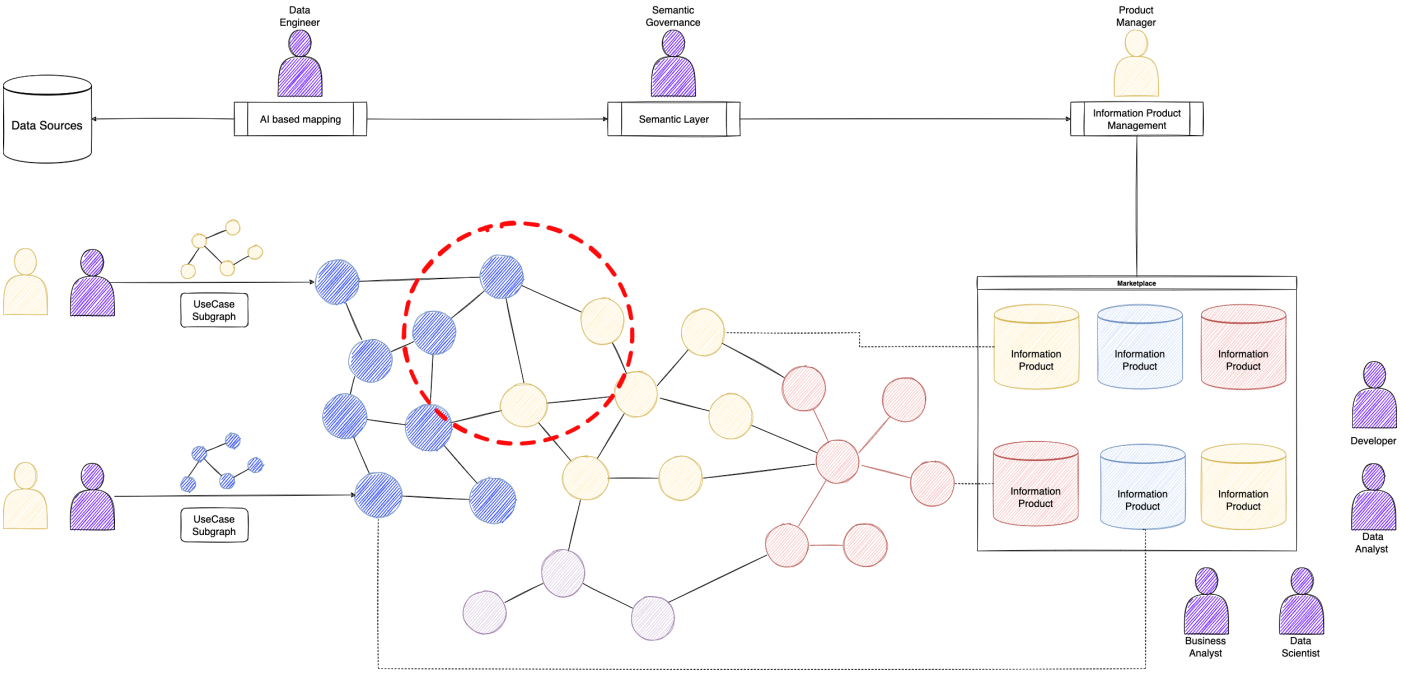


Figure 1 - Information Products by adorsys

Challenges in Modern Data Management

fragmented, poorly documented data across departments, leading to inefficiencies and duplication. Without a unified approach, reconciling data for a complete view of customers or operations becomes time-consuming and error-prone. Governance, security, and regulatory complexities further hinder progress. Regulations like GDPR impose strict rules, causing hesitation in data sharing and slowing innovation.

Additionally, a shortage of professionals with both technical expertise and a product mindset limits progress, while legacy IT infrastructure makes data retrieval cumbersome and market response sluggish.

Evolution of Data Architectures

These challenges stem from the natural evolution of data management. Initially, Enterprise Data Warehouses (EDWs) centralized structured data for business intelligence but lacked scalability.

Data Lakes emerged to store vast amounts of diverse data at lower costs, yet poor governance often led to data swamps. The advent of Data Mesh introduced a decentralized model, aligning data ownership with business domains to enhance scalability and agility. However, adoption required cultural and organizational changes, including upskilling teams and establishing governance frameworks.

The Next Step: From Data to Information

To maximize data potential, organizations must shift from treating data as a product to delivering context-rich, actionable insights. This transformation requires embedding metadata, ontologies, and business rules to ensure information is meaningful for decision-makers. Unlike traditional data products, information products enable interoperability across business domains, breaking down silos and fostering collaboration. Governance and data quality are essential for accuracy, reliability, and regulatory compliance. A culture of data sharing is crucial, shifting from risk aversion to viewing information as a strategic asset. AI and advanced analytics further enhance information products, providing predictive insights and competitive advantages.

Implementing an Information-Centric Architecture

As shown in figure 1 - Information Architecture by adorsys is our approach to transform systematically from data to information. A structured approach is vital for transitioning to information-driven decision-making. Key steps include assembling the right team of data engineers, semantic experts, and information product managers. Cross-functional collaboration ensures business ontologies are well-defined and aligned with strategic goals. A linked data platform enforces enterprise-wide standards and facilitates integration. High-quality data transformation combines machine learning with human expertise to improve accuracy over time. A centralized information product management platform oversees access control, security, and discovery of semantic data assets. Beyond technology, fostering a data-driven culture requires training, collaboration, and early wins to drive adoption. Continuous feedback, performance monitoring, and iterative improvements ensure long-term success.

Conclusion

Data is the foundation for innovation and growth, but unlocking its full potential requires a strategic shift. By learning from past evolutions and investing in the future, businesses can transform data landscapes into thriving ecosystems that deliver exceptional value. The transition from data-driven to insight-driven strategies will define the next era of enterprise success. Those who embrace this transformation will gain a competitive edge, improved decision-making, and a strong foundation for long-term growth.

Tim Biedenkapp
Director Information Management & AI
adorsys GmbH

Detailed information in the techL profile: adorsys

The need for an overarching AI implementation strategy in the company: A guide to successful implementation

An article by Sascha Sambale, Bosch Digital

In today's era of digital transformation, the integration of artificial intelligence (AI) is a key challenge for companies in all sectors. The question of the need for an overarching AI implementation strategy can clearly be answered in the affirmative. Such a strategy not only offers efficiency gains, but also lays the foundation for sustainable success in the digital age.

From vision to implementation: AI as a strategic game changer

Implementing AI requires a holistic approach that involves all levels of the company. The starting point is the management level, which must formulate a clear vision for the AI-supported future of the company. The aim is to adapt the corporate structure so that AI-based processes can be seamlessly integrated, but above all to optimize existing processes so that they can withstand the speed of this new technology.

When developing an AI strategy, the following key questions must be answered:

- What are the specific goals of the AI implementation?
- Which processes are to be automated? What new opportunities can be opened up by AI?
- What risks and dangers need to be considered?
- What impact will the introduction of AI have on employees?

Answering these questions provides the compass for developing a comprehensive and targeted AI strategy. It is important that the strategy not only considers technical aspects, but also incorporates organizational and cultural changes.

Define and analyze fields of action: AI as a tool for transformation

In the first step of AI implementation, a detailed analysis of the possible applications is essential. Not every process benefits equally from AI-supported automation. Companies must carefully consider in which areas the use of AI makes sense and where traditional working methods are still more efficient. Even if there is an urge to use this new technology everywhere, a thorough cost-benefit analysis is essential.

This strategic analysis forms the basis for selecting the right AI tools for the identified business areas. The market offers a wide range of AI solutions, but not every tool is equally suitable for all companies and all business areas. A careful selection that is tailored to the specific needs and requirements of the company is crucial in order to achieve maximum efficiency and added value.

Among other things, it is crucial to carefully weigh up when the flexibility of the tool should be preferred over a simpler user experience - depending on the area of application and the target group. To support this process, some companies have already taken proactive steps. For example, Bosch has asked all divisions to identify and prioritize potential use cases for AI. This bottom-up approach makes it possible to utilize the expertise of

associates while ensuring that the AI implementation meets the actual needs of the company. Based on the collected use cases, areas of application could be quickly defined and the most important tools prioritized.

Tool selection and rapid development: AI as a dynamic process

The field of artificial intelligence is developing at breathtaking speed. Companies need to adapt to this dynamic and adjust their processes accordingly. This applies in particular to the onboarding of new AI tools and the integration of new AI-based applications.

The ability to adapt quickly to technological changes is a key factor for the success of an AI strategy. Companies should build agile structures to quickly evaluate, test, and integrate AI technologies into existing processes.

Companies should consider the following aspects when selecting and implementing AI tools:

- Compatibility with existing systems and processes.
- Scalability and adaptability to future requirements.
- User-friendliness and acceptance by employees.
- Data security and compliance with existing regulations.
- Cost-benefit assessment to identify potential savings.

An effective AI strategy must also leave room for experiments and pilot projects. By implementing AI on a small scale, including through Proof Of Concepts (PoC), companies can gain valuable experience and identify potential challenges early on before considering a company-wide rollout. I often convey the principle in business units: “Experiment with this technology. Experiment with what you find online. If you recognize that it is useful for our company, we will evaluate the tool, model or service and possibly add it to our portfolio.”

Increasing efficiency and ROI: AI as a lever for efficiency and employee satisfaction

A successful AI strategy goes far beyond simply increasing efficiency. It aims to improve the quality of employees' work and relieve them of repetitive tasks. AI can offer employees valuable support by automating routine tasks and giving them more time for creative and challenging activities - something that cannot be calculated in monetary terms for the time being.

This approach not only increases productivity, but also the satisfaction of employees who feel motivated and supported by working with AI-based tools. Internal studies have shown that employees who perceive AI as a supportive tool have a higher level of job satisfaction and commitment.

It remains essential for the company that the use of AI ultimately brings financial added value. When calculating the return on investment (ROI), companies must analyze various use cases. This is not only about financial savings, but also about qualitative factors such as:

- Save time by automating routine tasks.
- Improving the quality of decisions through data-supported analyses.
- Increasing innovative capacity by freeing up creative resources.
- Increased customer satisfaction through faster and more precise services.
- Reduction of external expenditure through higher quality preliminary work within the company.

A holistic ROI analysis takes into account both

short-term efficiency gains and long-term strategic benefits resulting from AI implementation.

Data security and ethical aspects: AI as a trustworthy technology

Protecting sensitive data is crucial for AI adoption. Companies must ensure that the processing of data by AI tools complies with data protection guidelines.

The following questions must be clarified transparently:

- Where does the data processing take place?
- Who has access to the data?
- How is the data protected against unauthorized access?
- Does the company have guidelines regarding data protection classifications?

These aspects must be an integral part of the AI strategy, just as they were when cloud technologies were introduced. However, a key difference is that with AI applications, it must be contractually stipulated that sensitive data will not be used to train the models and may be shared with other companies. Consequently, one element of the strategy should be to consider whether data processing can be realized in the cloud or whether a local AI stack may need to be implemented in the company for some of the data.

Additional challenges arise in the area of generative AI. The models used have been trained with data that may be protected by copyright. Although the content generated by the models is created spontaneously and does not initially fall under copyright law, it is possible that copyrighted texts or graphics may be generated. Companies must be aware of these risks and establish processes to be able to react in the worst-case scenario or to minimize these risks in advance. An important part of the corporate strategy is therefore the development of guidelines and basic principles for the use of generative AI.

The use of AI technologies will shape the working world of the future and ethics are therefore of essential importance when implementing artificial intelligence. Companies must ensure that AI-based decisions are fair and transparent and do not cause discrimination. The same applies to the usability of the respective AI application. It is crucial to involve the works council at an early stage in order to familiarize employees with upcoming innovations and clarify any reservations. Within large organizations with existing works council structures, it is essential to anchor the implementation of artificial intelligence as an integral part of the strategy, which includes documenting decisions and regulations as part of a group works council agreement.

Training and further education: AI as an opportunity for the future

Comprehensive employee training is an essential component of a successful AI strategy. Employees must understand AI's opportunities, limitations, and risks to use its tools effectively and securely. Internal studies have shown that employees who are trained in the use of AI work more efficiently and can make better use of the technologies. Specially designed training programs can facilitate the use of AI and strengthen confidence in the technology.

- A comprehensive training program should cover the following aspects:
- Absolute basics of AI to understand the basis and background
  Specific training for the AI tools used in the company.
- Legal and ethical aspects and responsible use of AI.
- Data protection and security aspects when working with AI.

Targeted training ensures that employees are able to use the new tools effectively and safely and thus contribute to the overall success of the company.

Conclusion

A comprehensive AI implementation strategy is essential for companies in the digital age. It enables the effective use of AI potential, increases efficiency and employee satisfaction and at the same time takes ethical and data protection aspects into account.

A well thought-out AI strategy includes:

- A clear vision and objective for the use of AI for the entire company.
- Careful analysis and selection of suitable fields of application and tools.
- Agile structures for rapid adaptation to technological developments.
- Consideration of data security and ethical aspects.
- Comprehensive training and development programs for employees.

By implementing such a strategy, companies can not only achieve short-term efficiency gains, but also secure their long-term competitiveness and open up new business opportunities. A well-thought-out AI strategy forms the foundation for a sustainable and successful digital transformation of the company.

Sascha Sambale

GenAI Lead
Bosch Digital

Overcoming inefficiency and legacy system constraints

Struggling with inefficiencies, rigid legacy systems, and slow innovation cycles? Discover how low-code solutions can transform your processes, modernise systems, and rapidly respond to market changes, ensuring sustained competitiveness.

An article by Silvan Stich, Zühlke

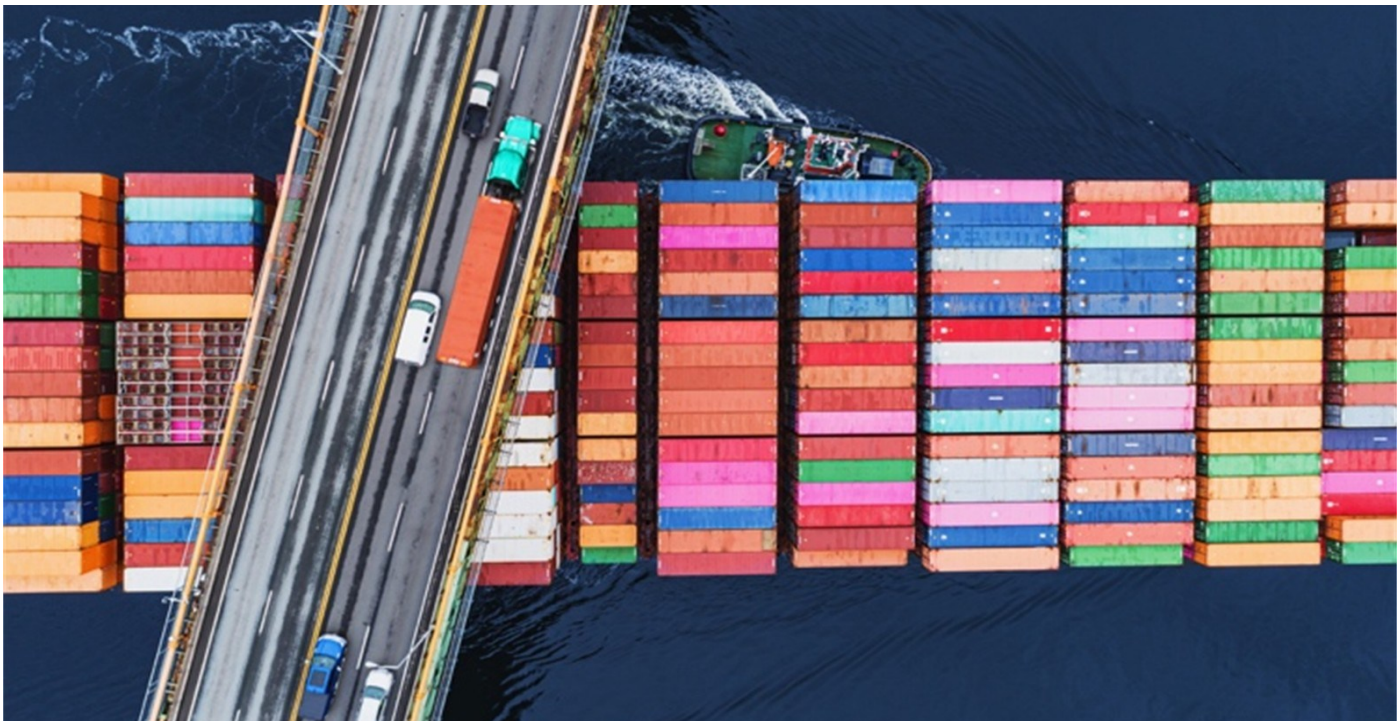


Image credits: Zühlke Engineering GmbH

Low-code platforms empower organisations to digitise processes quickly, modernise legacy systems, and drive innovation, reducing costs and strengthening long-term competitiveness. Learn how low-code can position you ahead by accelerating digital transformation and enhancing responsiveness.

Low-code platforms enable teams to rapidly create powerful software solutions, from simple productivity tools to mission-critical enterprise applications. This approach significantly reduces costs, accelerates digital transformation, and enhances your organisation's ability to meet both internal operational needs and external customer expectations effectively.

Today's businesses face increasing pressures from economic uncertainty, rapid technological advances, and changing consumer demands. Innovations like Artificial Intelligence (AI) and the Internet of Things (IoT) are transforming how businesses operate, making it essential to stay agile and responsive. Organisations must continuously evaluate and adjust their products, services, and internal processes to remain

competitive. Low-code solutions enable companies to quickly adapt to these shifts by simplifying and accelerating innovation.

Many companies still depend heavily on manual processes, which are often slow, prone to mistakes, and inefficient. Low-code solutions help automate routine tasks, such as administrative duties and customer service interactions, drastically reducing errors and freeing staff to focus on more valuable tasks.

For example, SWICA, a leading Swiss insurer, used the Mendix low-code platform to transform its slow and manual quotation process. Working with Zühlke, SWICA rapidly automated this process, significantly cutting quotation preparation times by 30-50%. This case highlights how low-code can effectively streamline critical business operations.

Outdated legacy IT systems often limit a company's ability to innovate. These older systems can be expensive to maintain, difficult to upgrade, and slow to adapt to new requirements. Low-code technology supports a structured approach to gradually modernise these systems. Starting with careful business analysis, low-code platforms make it easy to build new applications that integrate smoothly with existing technologies. Continuous platform updates ensure solutions remain modern, reducing the ongoing maintenance burden.

Low-code platforms are particularly suited for projects needing fast results and user-friendly designs, such as routine application development, legacy system migrations, and digitising disjointed or manual processes. They offer significant advantages for projects under tight deadlines or with high expectations for ease of use.

Choosing the right low-code platform involves aligning it closely with your specific business and IT needs to ensure it delivers maximum value quickly and efficiently.

To effectively manage organisational changes, it's crucial to integrate low-code solutions into your overall transformation strategy. Combining business analysis, thoughtful customer experience design, and expert software practices with agile methodologies ensures sustainable improvements. Looking forward, generative AI will further enhance low-code capabilities, enabling even faster software development, intelligent process recommendations, and improved user experiences, thus significantly accelerating innovation and efficiency.changes. Additionally, they complicate the introduction of new technologies essential for competitiveness. A structured approach to gradually modernising these systems is indispensable.

Silvan Stich
Head of Low Code
Zühlke Engineering GmbH

Detailed information in the techL profile: Zühlke

Agentic AI: Leading the Charge in Legacy Modernization and Rapid Software Development

Agentic AI represents not just an upgrade, but a paradigm shift. The potential extends far beyond the immediate benefits of cost reduction and faster project timelines.

An article by Agnes Bührmann, Publicis Sapient

In the world of digital transformation, agentic AI is emerging as a game-changer, poised to revolutionize how businesses modernize legacy systems and accelerate the software development lifecycle. Imagine AI that not only assists but autonomously makes decisions, executing tasks without human intervention. This is the promise of agentic AI - a technology that can redefine efficiency and innovation.

Understanding Agentic AI

Agentic AI is more than a buzzword; it represents a shift in how we work and make decisions. Unlike traditional AI, which offers recommendations, agentic AI acts independently, automating complex workflows. It's like a self-driving car navigating its path, managing tasks traditionally controlled by humans. This autonomy is what sets agentic AI apart, offering businesses the potential to optimize workflows, reduce costs, and enhance responsiveness.

The Business Case for Agentic AI

Why should businesses care about agentic AI today? The answer lies in its ability to transform digital business transformation (DBT). By integrating agentic AI, organizations can streamline processes, enhance customer experiences, and drive innovation. For instance, imagine an AI that not only routes queries more effectively but also engages with customers to solve issues in real time. This capability can significantly reduce response times and boost satisfaction.

Accelerating Legacy System Modernization

Legacy systems, often burdened with obsolete code, pose significant challenges for businesses. Modernizing these systems traditionally requires substantial budgets and lengthy timelines. However, agentic AI redefines this equation by autonomously handling vast swaths of the development process. Imagine reducing a five-year, $40 million project to a 2.5-year, $16 million initiative - savings that free up capital for reinvestment.

Enhancing the Software Development Lifecycle

Agentic AI's impact extends beyond modernization. In the software development lifecycle (SDLC), AI can revolutionize how businesses build, test, and deploy software. With real-time code troubleshooting, deployment automation, and workflow management, AI transforms a sluggish process into a dynamic, iterative system. This means innovation happens faster, with fewer bottlenecks and more agile delivery.

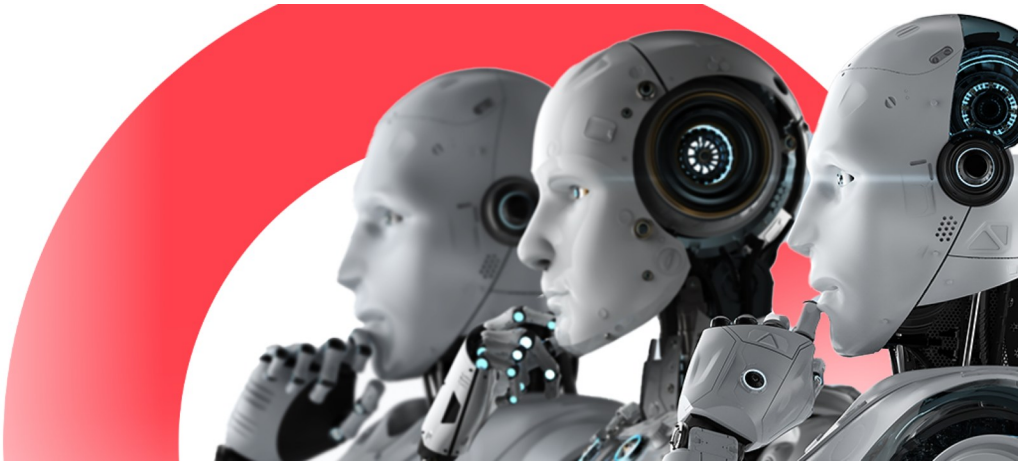


Image: Publicis Sapient

Navigating Challenges and Risks

While the potential of agentic AI is immense, it's not without challenges. Seamless systems integration is crucial for AI to function autonomously. Without it, AI's decisions could be based on outdated or incomplete information, leading to costly errors. Additionally, businesses must address risks like AI data poisoning and reward hacking. Implementing human-in-the-loop frameworks and using synthetic data can mitigate these risks, ensuring AI acts in alignment with business goals.

A Real-World Example

Powerful AI platforms like Sapient Slingshot offer a transformative opportunity for businesses across various industries by streamlining the software development lifecycle (SDLC). It is particularly advantageous for organizations aiming to modernize outdated systems, develop custom applications, or undergo MarTech transformations. This opportunity is crucial for businesses seeking to enhance operational efficiency, reduce time-to-market, and improve the quality of their software solutions. The platform supports code migration, documentation, and testing automation and provides a seamless integration with project management tools, enabling businesses to focus on strategic growth and innovation.

The Future of Agentic AI

As we look to the future, agentic AI represents a significant opportunity for enterprises. It's not just about automating tasks but about transforming how businesses operate. By embracing agentic AI, organizations can unlock new levels of efficiency and innovation, positioning themselves for success in an increasingly digital world. Agentic AI is set to redefine the landscape of digital business transformation. As we navigate this new frontier, the key will be to integrate AI thoughtfully, ensuring it aligns with organizational goals and delivers tangible value.

Agnes Bührmann
Industry Lead
Retail & B2B
Publicis Sapient

Detailed information in the techL profile: Publicis Sapient

Agentic AI: Artificial intelligence that independently orchestrates processes

How can IT efficiency be increased and automation driven forward? Agentic AI independently takes on tasks, optimizes processes, and seamlessly integrates into existing systems.

An article by Bastian Emondts, Campana & Schott

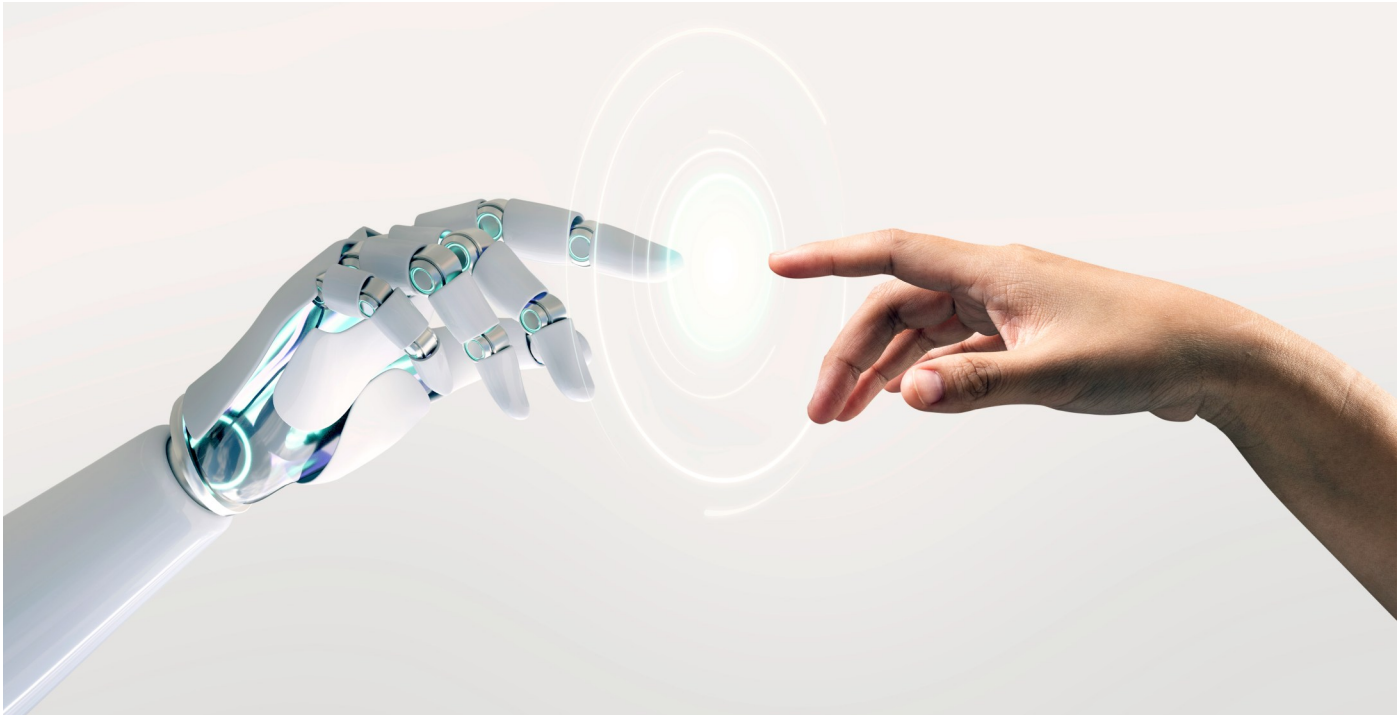


Image: Campana & Schott

Generative AI opens up new possibilities for departments, including text creation, idea generation, and assistance with day-to-day work. However, many tools are designed for direct human interaction. While they support employees with individual tasks, they usually do not automate processes. Agentic AI goes beyond this. It uses specialized AI agents that independently take on tasks, combine information from various sources, and autonomously initiate processes. For IT and other specialist departments, this creates the opportunity to make automation more efficient and decentralized.

Agentic AI supplements GenAI with autonomous action. Unlike traditional automation solutions, AI agents work contextually, access various data sources, and perform tasks throughout entire process chains. They interact with users, systems, and increasingly, with each other. Three types of agents can be distinguished in practice:

1. Retrieval agents search internal information sources and answer specific questions. For example, they are used in knowledge management, customer support, and checking guidelines.

2. Task agents take over specific work steps, such as filling out forms, writing texts, and initiating simple processes.
3. Autonomous agents work in the background to coordinate tasks and monitor processes, intervening when necessary.

An example from a communications department shows how AI agents can be used in practice: an agent takes over the routing of emails that are received via the central contact address. It recognizes applications and responds automatically with a reference to the career portal, forwards product inquiries to the relevant department and filters out irrelevant content. Employees save time, processes are accelerated and routine tasks are eliminated.

Networked agents are the next stage in the development of agent-based AI. They react to human input and communicate independently with other systems or agents, often using natural language. Unlike traditional integrations, which operate via clearly defined APIs, networked agents orchestrate processes dynamically and flexibly. For instance, a service agent could recognize a ticket with a cost reference and automatically instruct an SAP agent to make the booking. These types of scenarios are currently being tested and clearly demonstrate the potential of this new form of system integration. Rather than being rigidly linked via interfaces, processes would be designed using agent logic. This approach can avoid media disruptions, reduce integration costs, and enable companies to gain speed, modularity, and adaptability.

However, the use of agentic AI is changing not only technology but also the role of IT. AI agents can be seamlessly integrated into existing platforms, such as Microsoft 365, SAP, and ServiceNow, and implemented on this basis. This creates new possibilities: specialist departments can design their own processes while IT defines central standards, operates platforms, and ensures security. IT also becomes a consultant on the best ways to implement AI use cases. Some companies have already begun to support this organizational change by creating specialized teams that identify suitable use cases, implement pilot projects, and disseminate knowledge. Thus, agentic AI is not only a technological advance, but also a new organizational principle for collaboration between IT and business.

Agentic AI is not a distant vision. Companies that start with concrete use cases and existing platforms can quickly achieve noticeable effects. Large investments are not required; a clear understanding of the next step is sufficient. Initial agent solutions can be quickly implemented, and networked agents will enable more complex interactions and a new form of system integration in the future. Beginning this process now lays the groundwork for intelligent, adaptable automation closely linked to a company's strategic goals.

Bastian Emondts
Senior Manager
Head of App Innovation
Campana & Schott

Detailed information in the techL profile: Campana & Schott

Act now: The modern transformation from SAP ECC to S/4HANA - A practical guide

In a world characterized by digital innovation, the migration from SAP ECC to S/4HANA is a decisive step for companies. The paradigm shift in business software requires a timely and strategically well thought-out approach.

An article by Stefan Witt and Christoph Rump, Accenture

Free support for SAP ECC 6.0 will expire at the end of 2027. Originally, the end of 2025 was even on the cards, but SAP realized that most companies are sticking with the old version because they are afraid of the risks and effort involved in a migration. The reason for this is the typical mechanisms in companies that come into play when employees and end users have become accustomed to a system landscape after a long period of training, sweat and tears. The migration of such a fundamental program is risky, resource-intensive, associated with high costs and a long transition phase. Depending on the approach to migration, there are a number of challenges and pitfalls hidden from the willing company.

Due to the deadline for expiring support from SAP, but also in order to remain future-proof (in the cloud), the need for migrations to S/4HANA has increased massively in recent years. A distinction can be made between four approaches, which we will discuss in more detail below: Greenfield, Brownfield, Mix and Match, Empty Shell SDT.

We describe the different approaches in terms of their respective advantages and disadvantages with a focus on the quality assurance test-related measures during migration. For a successful migration, in addition to comprehensive planning and implementation and consideration of the above-mentioned transformation approaches, other aspects such as the possibilities of integrating test automation, the use of modern technologies such as artificial intelligence (AI) or specialized tools such as Accenture myConcerto should be considered. This article offers an insight into the various aspects of a modern transformation from SAP ECC to S/4HANA in order to provide companies with a practical guide.

Transformation approaches

Identifying the right transformation approach is crucial to the success of the migration. There are various strategies available to companies based on the initial situation, each of which has its own advantages and disadvantages.

Greenfield approach: In a greenfield project, companies start on a “greenfield site” by setting up and implementing a completely new system. This approach makes it possible to eliminate outdated processes and create an optimized and efficient system landscape right from the start. The downside is that the complete redesign can be time and resource intensive and there is a risk of losing proven processes and data.

Brownfield approach: The brownfield approach enables companies to transfer their existing data and processes to the new S/4HANA system. This approach is often less disruptive and enables faster migration, but carries the risk of adopting inefficient processes and data structures and

missing out on the potential for process redesign and optimization.

Mix and match: A hybrid strategy, which is a mixture of greenfield and brownfield approaches, allows companies to redesign certain processes while adopting others from the existing system. This approach offers a flexible solution, but requires careful planning and analysis to maximize the benefits of both strategies.

Empty Shell using SDT: The Empty Shell approach using Selective Data Transition (SDT) allows an empty S/4HANA instance to be created into which selective data and configurations are transferred from the ECC system. This offers maximum flexibility and control over the migration, but can be a complex and challenging task.

Test automation and the use of AI

The integration of test automation and the use of AI are key factors in ensuring system quality and efficiency during migration.

Test automation with Tricentis Tosca: Test automation tools such as Tosca play a crucial role in ensuring system quality. By automating repeatable test cases, organizations can save time, increase test coverage and improve migration quality. Following the philosophy of the shift-left approach, the use of such automation begins in the development stage during component or module testing. After successful manual testing, the individual components of the new solution are automated and continuously tested in a constantly growing regression test portfolio. This ensures that negative influences of modules to be developed on already completed modules are identified immediately. With an appropriate automation strategy, automated E2E process chains can be formed from these individual modules in the further course of a project, which can be used to carry out regression tests. Possible applications include regression tests in the run-up to a UAT for quality assurance or to secure instances that are already productive as part of a multi-stage roll-out (global roll-out in multiple waves). Due to the frequently incurred license costs for corresponding tools, the automation strategy should always also consider the use of the automation tools beyond the duration of the project.

AI for requirements generation and test cases: Depending on the deployment scenario, the use of AI can further optimize the migration process. For example, functional requirements for business processes described in a very free framework can be converted into structured requirements enriched with technical aspects using AI. Based on these structured requirements, the AI then generates the manual test cases for testing the previously described requirements in the next step. This improves test coverage and quality, while at the same time reducing the effort required to create test cases.

Use of Accenture myConcerto: Accenture myConcerto is an asset that provides the customer with a portfolio of several 1,000 both manual and automated SAP test cases that covers the existing SAP industry solutions. By providing ready-made test cases and centralized management of test cases and results, companies can make their test processes more efficient and improve collaboration in test management.

Advantages and disadvantages of the approaches

The choice of the appropriate transformation approach depends on various factors, such as the complexity of the existing system landscape, the specific business objectives and the company's willingness to rethink existing processes. While the greenfield approach enables a complete redesign, the brownfield approach offers a faster and potentially more cost-efficient option, but carries the risk of retaining inefficient structures. The mix and match approach offers a flexible solution but requires balanced planning to maximize the benefits.

The Empty Shell approach offers maximum flexibility, but presents companies with the challenge of carefully selecting the data and processes to be migrated.

Quality assurance and test management

Quality assurance and test management play a central role in migration. A comprehensive test strategy that is integrated into migration planning at an early stage is crucial for success. The integration of test automation and AI can help to increase the efficiency and effectiveness of the testing process. In addition, the use of tools such as Accenture myConcerto enables centralized management and monitoring of testing activities, which improves transparency and collaboration within the project.

Conclusion

The migration from SAP ECC to S/4HANA is a complex undertaking that requires careful planning and implementation. The choice of the appropriate transformation approach, the effective integration of test automation and AI, and the use of specialized tools are crucial to the success of the migration. By considering these aspects, companies can overcome the challenges of migration and take full advantage of S/4HANA to optimize their business processes and ensure their competitiveness.

Stefan Witt
SAP Testing Lead
Accenture Dienstleistungen GmbH

Christoph Rump
Quality Engineering Manager
Accenture Dienstleistungen GmbH

SOFTWARE INSIGHTS

United Innovations

SEP/OCT

17 SEP, 2025

GUIDE AND COLLECTION OF METHODS FOR THE INTRODUCTION OF DORA IN SOFTWARE TESTING

3:30 - 5 PM ONLINE

23 SEP, 2025

DIGITAL EURO: OPPORTUNITIES AND CHALLENGES ON THE PATH FROM THEORY TO PRACTICE

3:30 - 5 PM ONLINE

24 SEP, 2025

TARGET PICTURES IN ENTERPRISE ARCHITECTURE MANAGEMENT

3:30 - 5 PM ONLINE

01 OCT, 2025

LLM-DRIVEN ENTERPRISE LOWCODE AS THE FUTURE OF SW-DEVELOPMENT

3:30 - 5 PM ONLINE

09 OCT, 2025

AGENTIC AI

3:30 - 5 PM ONLINE

16 OCT, 2025

SUCCESSFUL APPROACHES TO DATA GOVERNANCE AND DATA ANALYTICS

3:30 - 5 PM ONLINE

21 OCT, 2025

AI POTENTIAL 2025 IN THE BANKING AND INSURANCE SECTOR

3:30 - 5 PM ONLINE

29 OCT, 2025

CLOUD - AUTOMATISIERTES ZENTRALES PLATTFORM MANAGEMENT MIT IAC (INFRASTRUCTURES AS CODE)

3:30 - 5 PM ONLINE

Navigating the Digital Operational Resilience Act (DORA): A Comprehensive Guide

How DORA is Reshaping Cybersecurity for Financial Institutions

An article by Matt Livermore, Perforce Delphix

The Digital Operational Resilience Act (DORA) represents a seismic shift for financial institutions operating within the European Union. Effective January 2025, this regulation seeks to bolster the cybersecurity framework of financial institutions, investment firms, and third-party ICT (information and communication technology) providers, ensuring they can withstand and recover from operational disruptions like cyberattacks or system failures.

Understanding and complying with the DORA requirements is crucial not only for regulatory adherence but also for staying competitive in a world of increasing cyber threats. Companies like Perforce are stepping up to provide robust tools and solutions to help meet these requirements.

What is the Digital Operational Resilience Act (DORA)?

The primary objective of DORA is to strengthen operational resilience across Europe's financial landscape. It consolidates legacy ICT frameworks under a unified mandate, creating consistency and improving effectiveness. Specifically, DORA focuses on four key areas:

- **Harmonizing ICT Regulations**: Moves away from fragmented standards, creating a uniform, EU-wide directive.
- **Strengthening ICT Risk Management**: Promotes robust frameworks for risk identification, mitigation, and recovery.
- **Enhancing Disaster Recovery and Reporting**: Improves organizational response to catastrophic failures and mandates clear, efficient reporting mechanisms.
- **Tightening Third-Party Vendor Oversight**: Calls for rigorous scrutiny of ICT service providers to ensure broader supply chain security.

For institutions that fail to comply, the consequences could range from significant fines to reputational damage.

Why Institutions Must Take DORA Compliance Seriously

With the introduction of DORA, financial institutions now face heightened scrutiny over their cybersecurity measures. Non-compliance puts organizations at risk of hefty penalties, potential breaches, and operational disruptions. However, beyond enforcing regulations, DORA presents an opportunity. By adopting its standards, institutions can build more resilient, efficient, and secure systems that bolster customer trust.

5 Key Capabilities for DORA

Perforce provides tailored solutions to bridge the gap between compliance mandates and

operational feasibility. Leveraging their technologies, financial institutions can address the specific demands of the DORA regulation.

1. Identifying Software Vulnerabilities

To comply with DORA, institutions must set up measures for continuous identification of software vulnerabilities.

2. Securing Infrastructure Against Risks

Beyond software, protecting hardware and systems from risks is equally critical.

3. Moving and Masking Sensitive Data

Moving sensitive data in compliance with DORA requires secure, cost-effective, and risk-managed systems.

4. Enhancing Downtime Recovery Time

The ability to recover from cyberattacks or outages is a key DORA mandate.

5. Speeding Up Forensic Audit Processes

After a disruption, DORA demands institutions conduct forensic audits to determine impact and remediation measures.

Practical Insights for DORA Implementation

While DORA's requirements may seem overwhelming, breaking them into actionable steps can simplify the path to compliance:

1. **Risk Assessment**: Conduct a comprehensive analysis of your ICT ecosystem to identify vulnerabilities.
2. **Vendor Management**: Start implementing more stringent evaluation criteria for third-party vendors.
3. **Automate Security Measures:** Use tools that continuously monitor and harden your infrastructure and software.
4. **Establish Reporting Protocols**: Build a system for clear, efficient communication of incidents to regulators.
5. **Invest in Scalable Solutions**: Ensure your systems are adaptable as business operations evolve.

Realizing the Benefits Beyond Compliance

Adopting DORA-aligned measures not only helps financial organizations comply but also creates additional advantages:

- Increased customer trust in secure, stable systems.
- A competitive edge in a dynamic industry.
- Long-term cost savings by implementing scalable, efficient cybersecurity solutions.

Reduce the Complexity of Compliance with Perforce

Building resilient systems while ensuring compliance doesn't have to be a daunting challenge. Technologies like Perforce Delphix and Perforce Puppet are purpose-built to simplify and streamline compliance efforts. They enable financial institutions to shore up system security, meet DORA's accountability requirements, and gain a firm competitive foothold in Europe's financial services market.

Matt Livermore
Director, Sales Engineering
Perforce Delphix

Detailed information in the techL profile: Perforce Delphix

Be prepared for emergencies with business continuity management

In the dynamic business world, companies are regularly confronted with unexpected disruptions and crises - be it due to natural disasters, technological failures, cyber attacks or human error. Such events can have a significant impact on the ability to do business and, in extreme cases, can even lead to a complete standstill. This is where Business Continuity Management (BCM) comes into play: a systematic approach to ensure that companies remain capable of acting in times of crisis and can resume their business processes as quickly as possible.

An article by Dr. Verena Pawolski, Materna Information & Communications SE

This white paper highlights the key aspects of effective BCM and provides a sound overview of how companies can prepare for emergencies. It presents proven strategies and methods for risk analysis and contingency planning to strengthen the organization's resilience and respond quickly to unexpected failures. Unprepared organizations are hit hard: a disruption can cause immense financial damage and also jeopardize customer trust. Find out how you can successfully establish and continuously develop BCM in your company to be optimally prepared in the event of an emergency. Prepare your company for unexpected business interruptions with the right measures to avert crises quickly.

Downtime in the worst case

Unexpected outages are inevitable in every company. Although it is impossible to predict the time, type or location of such an event, it is certain to happen at some point - whether due to technical failure, human error, malicious intent or simple bad luck. It becomes critical when such a failure is so serious that it becomes an emergency. An emergency occurs when the malfunction can no longer be rectified by the usual means and the company is significantly impaired as a result.

Fortunately, such serious events rarely occur. Nevertheless, organizations can only minimize the risk of downtime, but not completely eliminate it. One thing is certain: when a crisis occurs, it must be dealt with as quickly as possible, as the longer the business interruption lasts, the greater the negative impact.

In order to be able to react quickly and effectively in an emergency, comprehensive information, careful preparation and regular exercises are essential. This may involve considerable effort, but it is essential to ensure the company's resilience.

Information:

Extensive knowledge and understanding of your own organization is required in order to be able to adequately assess an emergency situation. Only then can companies react appropriately to the emergency situation that has occurred. To do this, those responsible must have a precise understanding of their own processes, their resources and dependencies and know the

associated services. Up-to-date information about assets is crucial, for example about how they interact with each other and what they are used for. This is only possible if access to a well-maintained CMDB (Configuration Management Data Base) is available. In conjunction with an IT service management or enterprise service management system, this information is also an essential part of day-to-day incident management. If organizations also handle emergencies in such a system, they can use the same information base. In addition, the responsible organizational unit (depending on the organization, the BC manager or the crisis team, hereinafter referred to as the BCM team) can recognize the transition from an incident to an emergency in good time and coordinate the measures to be taken.

Preparation:

In order to prepare for an emergency, various questions need to be clarified. The most important of these is which business processes need to be restored in which time frame following a potential total failure. This also includes knowing which failed business processes will severely disrupt the company's ability to do business. In order to generally avoid such a disruption to business capability, those responsible for BCM should assess and monitor the corresponding risks. With suitable measures, they can reduce their probability of occurrence or impact. It makes sense to plan targeted measures that limit the damage in the event of an emergency and create valuable time for recovery.

It is equally important to analyze possible emergency scenarios in advance and develop concrete emergency plans. These plans define clear steps that are required to restore operational capability. Those responsible also define the sequence of tasks and designate the persons responsible in each case. In an emergency, the BCM team also draws on prepared fallback processes and coordinated communication strategies in order to react quickly and in a coordinated manner.

Practice

Drills and tests help to ensure that action can be taken quickly in an emergency. They ensure that everyone involved knows what to do and that the technology is proven to work. Everyone involved thus acquires a certain routine in emergency response and interaction with each other. Regular practice also has a valuable side effect: emergency plans are reviewed in advance and can be improved and further developed.

Well prepared with structural planning

All these preparations are crucial for effective and reliable emergency planning. If important information is missing, the company runs the risk of creating incomplete or incorrect planning. If the BCM team makes incorrect assumptions in the analysis phase, this can lead to business incapacity in an emergency. If information, training and practice measures are neglected, valuable time is lost as the employees involved must first be familiarized with the new processes and tasks.

In addition, European regulations such as NIS2 and DORA also require companies that are part of the critical supply chain to have a functioning risk management and emergency planning system. Companies that take care of their business continuity management now will be one step ahead of future directives and secure a competitive advantage.

Business continuity management helps

Business continuity management (BCM) takes all of the above points into account, documents them and puts them into practice. With the help of a business impact analysis, those responsible analyze existing services, processes and resources in terms of their relevance to emergencies. They use a risk analysis to develop and

establish preventative measures and then develop, review and refine emergency plans. These are extensive processes that permeate many areas of the organization. Setting up these processes is initially time-consuming and resource-intensive. However, these processes and the time invested in them are indispensable in an emergency and protect the organization from far-reaching damage.

Necessary steps for setting up business continuity management

First and foremost, a declaration of intent is required from top management. In addition to the provision of personnel and budget, it is important to define far-reaching strategies and directions. This sets the framework for BCM, as the usual company organization is turned upside down during an emergency.

1. business impact analysis

A good start is to carry out a business impact analysis. This involves discussing business processes one after the other with regard to their flow and the consequences of an outage. The BCM managers specifically address the expected damage of an outage to the organization and put this into a time frame. The business impact analysis determines how long a service outage can still be tolerated before it significantly impairs the business capability of the entire organization. The time determined in this way forms the maximum tolerable downtime. It is a measure of the time in which a service must be available again and is determined by the economic consideration of the total outage. A business impact analysis also shows which emergency operations can be maintained from a business perspective and which additional measures should be taken to delay significant damage to the organization after an outage and provide the recovery team with more time.

The time it takes for organizations to be fully operational again after a critical incident can vary greatly and depends on several factors. These include the nature of the incident, the size of the organization and the effectiveness of contingency plans. The good news is that well-prepared organizations with robust contingency plans and regular testing of their recovery processes are usually back up and running faster.

2. contingency planning and emergency coordination

Contingency plans are instructions that describe exactly what needs to be done to get the failed system back up and running. Overall coordination is the responsibility of the emergency response team. This relies on good preparation - especially as the actual implementation of the emergency plan is usually the responsibility of the technicians. Regular tests and exercises help to ensure that everyone involved is familiar with the situation-related tasks. The control of the individual activities, their monitoring, communication and logging are the essential tasks of the emergency response team and should be efficiently supported by a tool, especially in an emergency situation.

3. risk management

The task of risk management is to identify, assess, treat and monitor vulnerabilities. In the context of BCM, this relates to risks which, if they occur, would massively disrupt the normal functioning of assets, services and business processes. If risk management succeeds in taking suitable measures to prevent or reduce the impact of such events, it makes a decisive contribution to preventing emergencies. Furthermore, it is essential that identified risks, measures taken and emergency plans in place build on each other.

4. Organizational framework conditions and processes

BCM does not function in isolation, but interacts with various IT processes, with incident management

- i.e. troubleshooting - playing a central role. A failure is usually perceived as a fault and reported. The processor then needs information to identify which business process is affected and how critical this process is for the organization. This is the only way to convene the emergency team as soon as it becomes apparent that the disruption is an emergency due to its extent and urgency. For this to happen reliably, all relevant information on the failed system must be accessible. There must also be a clearly coordinated process for reporting and notifying the emergency response team.

5. emergency scenarios

All preparations are bundled in emergency scenarios. These scenarios are developed based on a high risk of occurrence. In such a scenario, reporting processes and alerts are tailored to the specific case, taking into account the various emergency plans of individual systems and the time available, depending on the business processes affected. In this way, the interaction of all individual steps and components is already thought through and practiced when the emergency occurs.

How to set up successful business continuity management

Materna offers OpenText Service Management as an established solution, which offers users decisive advantages as a BCM tool. The tool simplifies the entire process of planning, monitoring and restoring business processes in the event of a failure thanks to its clarity. The system offers structured processes and enables effective incident management. One of the most important functions is the automation of emergency processes. OpenText enables the automation and orchestration of business processes, resulting in a faster response in the event of an emergency. Prepared workflows can be activated immediately to restore critical IT services quickly. In addition, the system supports risk management by identifying potential risks and implementing risk mitigation measures. It also ensures comprehensive documentation and traceability, which is essential for audits and the continuous improvement of processes. By promoting integration and collaboration between different departments, OpenText helps to ensure that an organization can respond quickly and effectively in the event of incidents and maintain business continuity.

BCM expert team

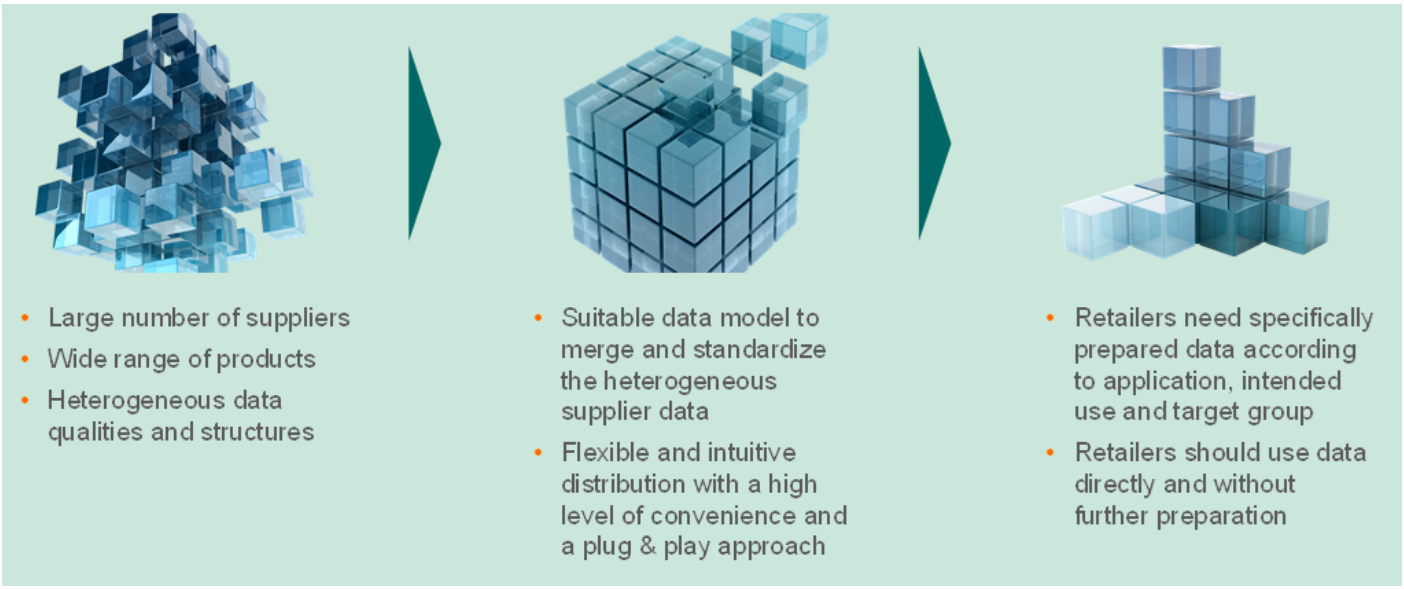
Materna is an experienced service provider and German market leader for ESM solutions and technologies. Materna offers OpenText Service Management as an established solution, which also fully maps BCM. This enables a comprehensive and integrated solution for the management of business interruptions. With well over 1,000 successfully implemented projects and around 30 years of experience in the field of ESM and as a Platinum Partner of OpenText, Materna has extensive expertise in advising and supporting highly diverse organizations in establishing their business continuity management. Materna has a well-trained competence center for OpenText products and comprehensive technology know-how that enables it to develop and offer advanced solutions. The extensive process know-how of the OpenText software products ensures that the solutions are optimally tailored to the needs of the customers. In order to meet individual requirements, Materna relies on tried-and-tested best practices during project implementation, thus guaranteeing efficient and successful implementation.

Dr. Verena Pawolski
Senior Consultant
OpenText Consulting Services
Materna Information & Communications SE

Automating data management with AI: success factors

High-quality data is the basis for increasingly relevant digital sales and efficient procurement processes and has a direct impact on business results. Retailers today need comprehensive and permanently up-to-date product data for the various sales channels used in order to serve the needs of their target groups and achieve customer loyalty. But how can these goals be achieved with constantly growing product ranges, accelerating innovation cycles and less reliable supply chains? This article uses the example of E/D/E data management to show how AI can be used to automate data processes and significantly increase performance.

An article by Jürgen Pannek, Einkaufsbüro Deutscher Eisenhändler



What are the key challenges associated with product data management?

Most of the challenges revolve around **data collection** and **data distribution**:

- In industries with diverse manufacturer and supplier structures, retailers are faced with the challenge of **maintaining a wide range of products**. Today, extensive and high-quality product data is required for the various suppliers with a wide range of products (e.g. tools, factory equipment, welding technology, construction, personal protective equipment, technical trade, building services, steel). However, retailers are confronted with **heterogeneous data qualities and structures** and have to manage this complexity. As individual retailers are less and less able to meet the data requirements, they are turning to partners such as the Einkaufsbüro Deutscher Eisenhändler (E/D/E).

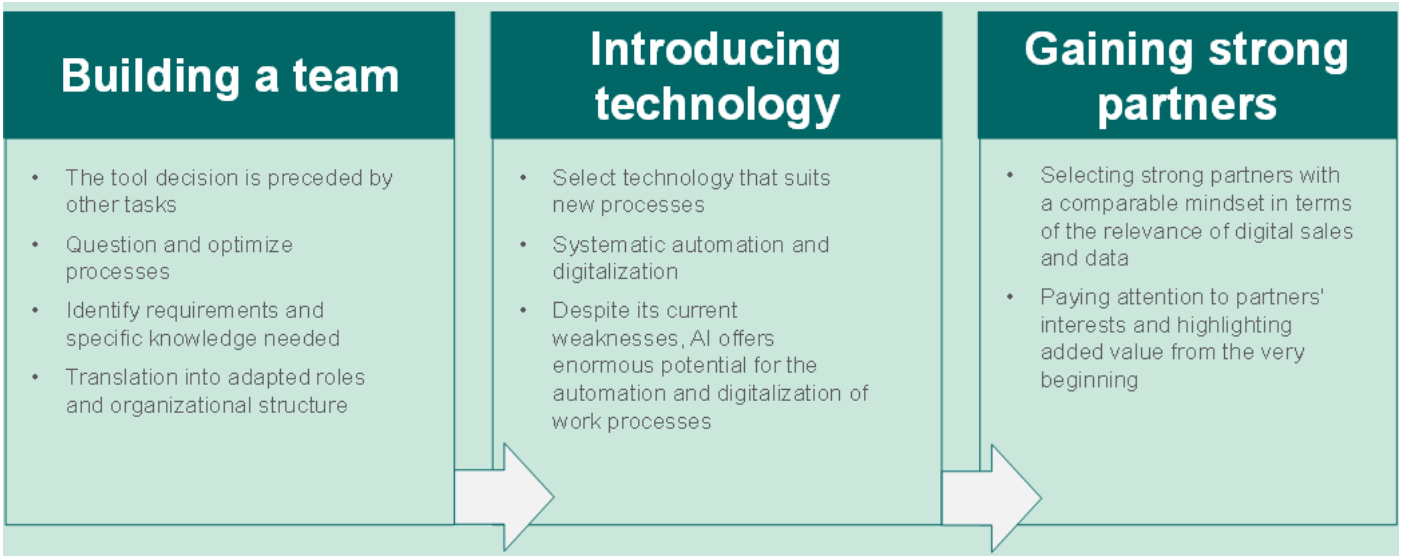
- **Data distribution** is a challenge in that end customers use a variety of channels for information and procurement as part of their customer journey. These channels must be played with **high-quality data in order to keep the platforms relevant**. On the other hand, if data does not meet customer needs, information and procurement platforms are quickly discarded permanently. Against this background, **specifically prepared data is required for the target channels** according to application, intended use and target group.
- In between lies the challenge of developing **suitable system architectures** and **data models** that meet the requirements in question. For E/D/E, for example, this means bringing together the product and marketing data of approx. 3.200 contract suppliers, standardizing it and making it usable according to the specific requirements of approx. 1.200 retailers.

Success story: Automated data management with the help of AI applications

Achieving a highly automated data management process **requires much more than the introduction of AI applications**. On the way to next-generation data management, E/D/E has developed an **implementation process based on 3 steps**, which are described below along with their **challenges, lessons learned and success factors**.

Step 1: **the team**

- **Uncertainty and fear of change** initially led to skepticism and defensive attitudes among the teams. One of the first tasks was to counteract fears of change and concerns about excessive demands.
- **Regular and transparent communication** about changes reduced uncertainty and enabled employees to ask questions and provide feedback. **Training** has prepared them for new technologies and increased their confidence. **Mentoring and coaching** have supported adaptation to change and promoted resilience. **Flexibility and co-determination** in change processes have strengthened the sense of control and belonging. **Regular recognition and appreciation of performance** have increased employees' confidence and motivation.
- With the necessary **mindset for more willingness to innovate and self-confidence**, difficult questions about process and structural changes can also be tackled. Ultimately, it has been shown that data management with automated processes and the use of AI requires **new organizational design in terms of profiles, roles and responsibilities**. On the other hand, this opens up a multitude of opportunities for the entire organization.



Step 2: **Technology selection and introduction**

- The focus of technology selection was always on the **company's own processes** and **specific industry requirements**
- Consistent automation and **digitalization of work processes** e.g. product classification, attribute mapping, content mining, content crawling, text generation at any time
- AI must be **carefully trained** and **requires interaction**. Automation cannot be achieved at the push of one button. There are always setbacks to deal with. High-quality and comprehensive data is essential for training. One million products for training are just the foundation. **Technology and business experts should work together to optimize the models**, as subsequent **corrections are time-consuming**

Step 3: **Gain strong partners**

- Select **strong partners with same aspirations** in terms of the relevance of digital sales and data
- Industry **interests considered** from the outset and added value highlighted
- Collaborative cooperation requires a great deal of **commitment and transparency** on all sides

In summary

The key findings from our data management automation journey can be summarized as follows:

- Challenges in data management are manifold. To achieve market impact, both **data collection and distribution must be ensured**
- Automation does not happen at the push of one button, **AI needs to be trained and requires interaction**
- More important than technology is the establishment of **sustainable processes** and an **innovative and open-minded organization**
- **Strong partners are needed both internally and externally** to overcome unavoidable obstacles

Jürgen Pannek
Director Digitale Services
Einkaufsbüro Deutscher Eisenhändler GmbH

Detailed information in the techL profile:
Einkaufsbüro Deutscher Eisenhändler

United Innovations

Survey of technologies

We regularly consult experts on their current needs, with tool research being a frequent request. Our techL database offers a curated selection of innovative technologies, including product summaries, detailed datasheets, and direct contact information — helping you find the right tools for your challenges.

All innovations be found in the technology database

techL

www.techl.eu

From Unlocking AI Agent Readiness with KNIME: Your Data Team Is Closer Than You Think

How can you start building truly agentic apps and systems, and turn your data team's know-how into a tool library to hit the ground running?

An article by Sasha Rezvina, KNIME

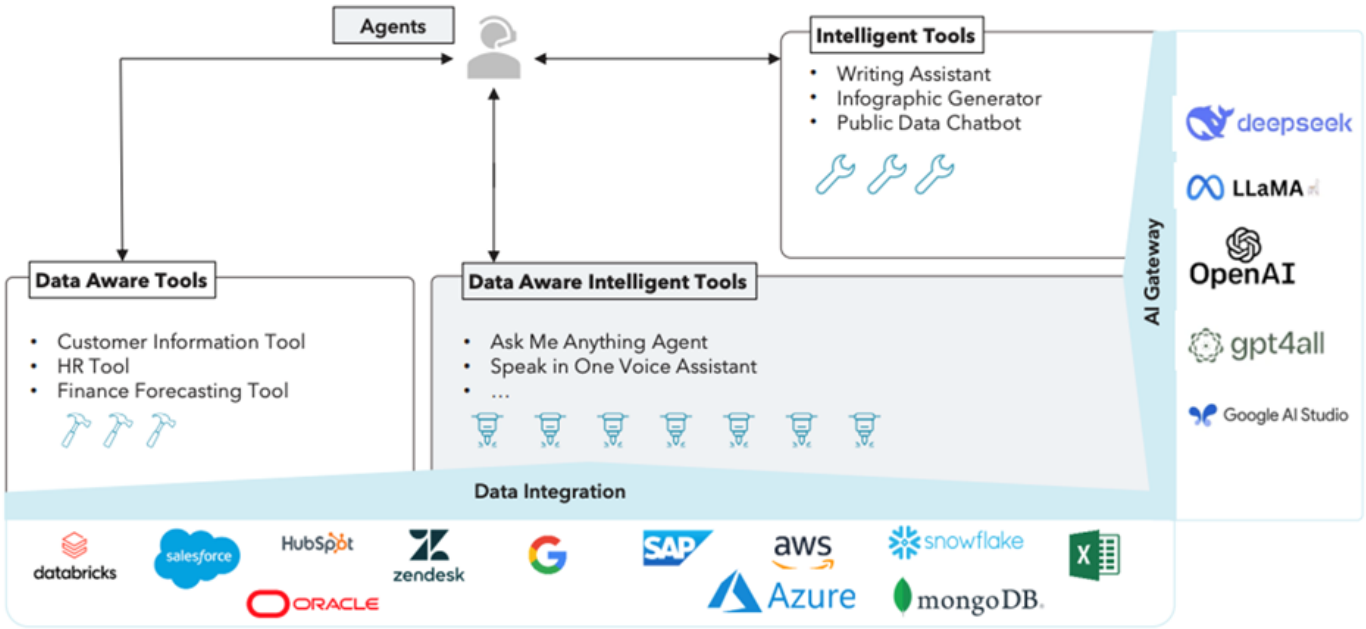


Image: KNIME AG

As organizations explore generative AI, many encounter a common set of limitations. Black-box LLM tools offer little visibility into how decisions are made. Vertical AI solutions often solve only one narrow use case. And while some low-code platforms promise ease of use, they sometimes struggle to provide the flexibility or traceability required for real-world, enterprise-scale solutions.

Data teams are finding limited value in only chatbots—they need to build systems that can take action. AI agents offer this next step, as systems that understand context, choose appropriate tools, and execute tasks with autonomy. The challenge isn't just building these agents—it's doing so transparently, with the systems, workflows, and teams you already have.

That's where KNIME fits in. Instead of forcing your data teams into new tools or rigid templates, KNIME enables your teams to build on the strength of their existing data infrastructure. With its visual workflow approach, open plat-

form model, and support for traditional, predictive and generative AI, KNIME enables your teams to build data-aware AI agents that are transparent, auditable and adaptable.

Building Agents with KNIME: Transparent, Practical, and Scalable

At its core, KNIME is a data analytics and AI platform. Its strength lies in its visual, workflow-based interface. Accessible to business analysts and data scientist alike, users can build and trace workflows step-by-step—making them ideal building blocks for agents.

These workflows can act as:

- **Tools** that handle specific functions (e.g., retrieving customer data),
- **Intelligent tools** that layer in LLM capabilities (e.g., summarizing documents),
- **AI workflows** that chain multiple tasks for more complex automation.
- **Agents themselves**

With KNIME, all these elements become part of a reusable toolset. Agents dynamically select and call the right tools based on a task's context—without needing you to hardcode every step.

Turning Existing Workflows into Agentic Infrastructure

Many organizations already have workflows for ETL, reporting, or machine learning. With KNIME, you don't need to be rebuild these—they can be reused directly as callable tools in an agentic system. Visual workflows become the "skills" agents can learn and deploy. With over 300+ connectors—from REST APIs and databases to cloud storage and LLMs—KNIME workflows can sit at the heart of your AI ecosystem.

KNIME also serves as a central repository where agents can browse, select, and execute tools. And KNIME Software supports the Model Context Protocol (MCP), making it easy to add on discoverable workflows and broaden agent capabilities over time.

Start Small, Scale Smart

Building your first agent in KNIME doesn't require a huge investment. Begin with simple workflows: a sentiment analyzer, a report generator, a customer lookup tool. Then link them. Let the agent decide which one to call, and when. Deploy it via KNIME Hub as a data app, service, or API. As you build more agents, they can call each other, share memory, and evolve into powerful multi-agent systems.

Agentic AI isn't a moonshot—it's a practical next step. And KNIME makes it transparent, modular, and aligned with how your team already works.

Sasha Rezvina
VP Marketing
KNIME AG

Low-code as an enabler for digital innovations in finance

Increasing regulation, growing customer expectations and rapidly changing markets are putting financial institutions under pressure to innovate. The modernisation of core systems, process automation and the development of new digital offerings and AI integrations often fail due to complexity and scarce IT resources. This is where low-code comes into play: the technology enables a paradigm shift in software development and promotes leaps in innovation in the financial sector.

An article by Benjamin Erschen, Mendix

With a powerful enterprise low-code platform, such as the one from Siemens company Mendix, the key challenges facing financial institutions in times of skills shortages, volatile markets and rising customer expectations in a digital world can be solved.

Low-code simplifies and accelerates application development through visual modelling using drag-and-drop functionalities, ready-made modules and interfaces.

The technology also democratises software development, as specialist departments and IT experts can work together on a single platform in fusion teams. This accelerates digitalisation projects immensely, as people outside the IT department can also contribute directly to development. This ensures that all applications are developed in a compliant manner and in accordance with the applicable security requirements, as all participants work within a framework specified by IT and with pre-defined governance.

Key areas of application for low-code

Low-code not only makes it possible to develop apps quickly and easily - whether in the cloud or on-premises - but also to seamlessly digitalise complex processes. Fragmented data silos can be merged and processes automated end-to-end.

Low-code unfolds its potential in the digitalisation of customer onboarding processes, the automation of internal inspection and approval workflows or the development of individual customer portals or self-service applications.

Whether onboarding or lending, the low-code platform from Mendix offers a wide range of tried-and-tested templates and connectors that can be seamlessly integrated into the existing technology landscape of financial institutions. The modernisation of legacy systems can also be implemented quickly with low-code, as it builds bridges - from existing core systems to new digital services.

More successful IT projects with low-code

Low-code offers financial institutions many advantages: The high development speed shortens the time-to-market and enables an agile response to market changes and regulatory requirements. Interdisciplinary teams relieve the burden on IT experts, who concentrate more on innovation-driven tasks instead of the IT backlog.

At the same time, IT costs are significantly reduced: for example, Rabobank reduced its budget by around 50 per cent when developing its new online portal with the help of Mendix. However, low-code not only saves time and money. Customised applications provide a significantly better customer experience than inflexible standard software, as they are tailored to specific customer needs.

AI and low-code ignite the innovation engine

Modern low-code platforms are AI-supported and ensure that users can utilise the productivity potential of AI and generative AI in a secure manner, allowing them to realise significant efficiency gains and develop intelligent applications based on the latest technology.

This is also underpinned by our study 'The Low-Code Perspective': 85 per cent of the 2,000 IT managers surveyed worldwide confirmed that the combination of low-code and AI helps them to innovate faster.

Business-critical relevance of low-code

Low-code is the strategic answer to the challenges of the digital transformation of financial institutions and meets the urgency of linking data sources from different core systems, digitising services across the entire customer lifecycle and developing innovative applications for increasing customer requirements.

Anyone who wants to play an active role in shaping digital change will find Mendix a powerful platform for implementing innovations in the financial sector more quickly, securely and efficiently.

Benjamin Erschen
Sales Director DACH
Mendix

Continuous Everything – Is the juice worth the squeeze?

Since years if not decades it is common sense in the software development community that things like integration / testing / delivery / deployment of software should be done in a continuous manner. But looking at the status quo there are still a lot of organizations which do not do this and if there are improvements planned in that area it is challenged if it is worth the investment. This article here should help every role involved in software projects to decide if the investment is worth it.

An article by Marco Achtziger, Siemens Healthineers

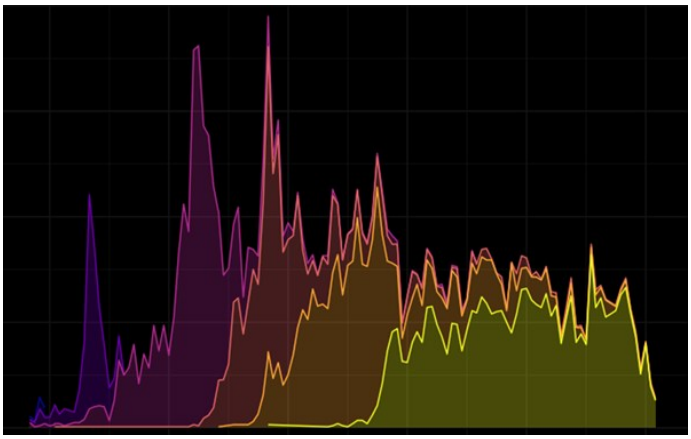


Image credits: Marco Achtziger

Already more than 10 years ago we started to automate more and more in the software development of an internal platform. That does not only mean testing but also other things like executing our builds in general and how often we make our packages available for further usage in our products.

Along the way there have been especially in the beginning questions like “What do we save by automating more tests/package generation/…?”. I asked myself that question too.

But first lets have a look at some things we changed to do things more continuously.

One of the first things we adressed was the execution of our builds. When we started we had a central build execution which generated only a few times per week new binaries. Of course developers build their changes locally but the whole compilation was only done in a low frequency. This caused that some things were found quite late in the full compilation. Nowadays we execute a build for every change which is done in our build system in a defined environment.

With executing the compilation more often we also wanted to ensure that it does not only compile but is also runnable. Therefore we automated almost all our tests and execute them. Now in our environment there is almost no build which does not execute automated tests in some way.

Having a lot of automated tests induced the next investment which had to be done. Especially the higher the test level you will find flaky tests. For us that means that a test shows a different outcome although it was executed on the same software baseline.

You cannot get rid of these tests completely but you should make sure that you can deal with them. What you want to avoid is the «Broken window syndrome» which means at the end that noone really looks at the builds because you

cannot trust them. The math here is simple and it means if you have around 8 tests which have a failure rate of only 10% in your system your build will fail with a 50% certainty.

Technically (despite of fixing the infrastructure or tests of course) we handle tests which are flaky but not easy to fix in a quarantine approach. So based on a defined process it is possible to take out the test for normal execution and run it in a quarantine environment. There it can be planned to fix it and bring it back to normal execution.

What you also must address for ensuring that people take care about the builds and tests continuously is the mindset. This cannot be done with setting up the builds and execution everything more often. This was additionally addressed with the introduction of so-called craftsmanship programs. These programs are free to join (so no team is forced to do so) and, as they define different levels, the teams can see where they can improve their skills and get better in what they do.

- Continuously doing things is not only a technical but also a mindset change
- You have to take time for it
- Make sure that you can measure your overall improvements

This is to make sure that really the behavior of the people changes. We follow here the pattern of Dan Pink mentioned in his book “Drive” where he states that you must give the people autonomy, mastery and purpose if you want them to change. This is especially needed in our white-collar environments according to Dan Pink.

What was also important in all these changes was that we do not make any difference between source code and test code development. Test code is treated as every other source code and has to follow the rules for the same. This ensures that the code can be read by developers and testers, and they can collaborate on the code base to improve for example the stability of the test cases.

As you can imagine doing these things (and these are only part of all the things we changed) are already quite some investments in the area of software development. So, question is if we can really measure the benefits of these.

Short answer is yes. What we looked at are the only two interesting metrics in our opinion: defects found and time needed for integrating changes of developers.

The image in the beginning shows our distribution of defects over time showing that we reduced the number of defects that we got significantly over the time. And with every defect less to analyze and fix developers have more time to implement now features.

Also the time to integrate software changes was reduced from several days in the beginning to less than 4 hours now (with an increase of the quality of course).

The impact on the defects alone already justifies quite some investment because when you look on the average time needed to solve a defect you can easily calculate how much time/money you save with every avoided one and you can provide a sum of total savings. Disadvantage is that these are lagging KPIs.

Coming back to the opening question: it is definitely worth doing the squeeze when it comes to software development and continuously doing things.

Marco Achtziger
Senior Software Architect
Siemens Healthineers AG

Future-Proof Synthetic Test Data

High-quality test data is the backbone of effective software testing. Yet, obtaining data that meets regulatory standards, aligns with business constraints, and remains scalable is a constant challenge. Many testers rely on production data—if available—or resort to costly workarounds. InputLab provides testers with a next-generation synthetic test data solution that eliminates dependency on real data while ensuring compliance, flexibility, and ease of use.

An article by Dominic Steinhöfel, InputLab

Image credits: InputLab GmbH

Software testers face a critical challenge: Sourcing high-quality test data. This data must support effective testing, accurately reflect business logic, and comply with stringent regulations like GDPR. The traditional approach, using laboriously pseudo-anonymized production data, comes with several problems. It's time-consuming, risks data leakage, and is infeasible for new applications or features, when testing is most crucial. Synthetic test data can help—if done right.

Software testers can choose between two fundamentally different options to source test data:

1. **Production Data Sampling:** This option comes with inherent privacy and security risks, even with appropriate data masking. Additionally, finding the *right* data between vast amounts of available production data is difficult. Ensuring consistency and keeping copied data up-to-date with changing systems adds another layer of complexity. For new use cases, this option is not even available.
2. **Synthetic Data Generation:** Many companies develop specific data generators for the use case at hand. Yet, these generators quickly

become unmaintainable and don't scale to complex requirements. It's no surprise companies only use them as *ersatz* production data. Recent AI-based approaches promise "production-like" data but introduce their own issues: trusting opaque AI models not to leak sensitive information is difficult, high-quality training data may not exist, and carefully curating this data to meet specific test goals without bias is a monumental task.

InputLab: Requirements-Driven Data Generation

InputLab provides a fundamentally different approach: schema-based synthetic test data generation built on transparency and precision. A spin-off of the renowned CISPA Helmholtz Center for Information Security (#1 cybersecurity research center worldwide) and backed by significant funding from the German Ministry of Research and Education, InputLab translates cutting-edge academic insights into industrial practice.

How InputLab Empowers Testers:

1. **Start Fast with Existing Specs:** Simply connect your interface specification, be it a database schema or XSD and Schematron files for a complex format like E-Invoices. InputLab automatically provides broad format coverage with minimal initial effort.
2. **Transparently Define Requirements:** InputLab makes it easy to incrementally add the business logic and semantic rules that truly matter. This specification becomes a clear, auditable model of your test data requirements, free from the biases hidden in production samples or opaque AI models.
3. **Generate Compliant Data On-Demand:** Produce data that adheres precisely to your defined structure and rules, ensuring GDPR compliance. Meet your specific testing goals, like edge cases, security testing, or negative testing. Since generation is driven by an explicit specification you control, trust is built-in.
4. **Adapt and Evolve:** Your data specification is no one-off script. It is an asset that adapts easily to evolving interfaces and new business requirements, ensuring your test data capabilities keep pace with development.

Proven in Practice

The InputLab approach has demonstrated its power and ability to handle complex, real-world data formats. For instance, it identified subtle bugs in major E-Invoicing software and contributed corrections to a European standard and the reference implementation by the German public service organization KOSIT. Only months after InputLab came to existence, early industrial partners are already leveraging InputLab to enhance their testing processes, validating its effectiveness.

Future-Proof Your Testing

Stricter privacy mandates? New regulations ("DORA 2.0")? New use cases and interfaces? With InputLab, you have a sustainable and adaptable test data solution. Instead of constantly reacting to new data challenges, you proactively define and generate the precise data needed, ensuring your testing remains robust and efficient well into the future. InputLab empowers you to move beyond data limitations and focus on what truly matters: delivering high-quality software.

Dr. Dominic Steinhöfel
CEO
InputLab GmbH

Detailed information in the techL profile:
InputLab

The rise of the hybrid tester

From typewriters to AI copilots, the evolution of software testing reflects the broader shift in how we work. As AI becomes a key tool in development, testers are transforming into hybrid professionals—combining human insight with machine speed. Embracing this change isn't just smart; it's essential for staying relevant and competitive in today's fast-paced tech world.

An article by Cristiano Caetano, Katalon

I'm pretty fast on my laptop keyboard, usually typing around 60 words per minute, sometimes even more, thanks to my mom. She signed me up for a typing course when I was 12 because she thought it would be useful for my career someday, years before I could get my hands on a real computer.

It turns out she was right, and it's still a handy skill today.

When I graduated from the typing course, my mom gifted me an Olivetti typewriter. It was amazing at the time! I ended up typing all my school assignments instead of handwriting them, which was probably for the best since my handwriting was terrible back then (and I guess it never really improved because of that).

Years later, even though I had been using DOS and Unix computers for a while, getting to use a mouse for the first time on Windows 3.11 and Word 6.0 was a magical experience.

Being able to print exactly what I saw on the screen, along with the ability to edit text instantly, was a game-changer, and don't get me started on the grammar and spell-check tools.

Word 6.0 and I became one, helping me work faster and better. Today, it's hard to feel those kinds of breakthroughs.

We live in a time where computers and mobile devices are incredibly powerful, GUIs are standard, and the internet has become essential like oxygen.

At that time, office productivity tools were just starting to become mainstream: word processors, spreadsheets, Xerox machines, fax machines, and more. It was a big leap forward in terms of productivity and efficiency.

With the rapid growth of AI today, it feels like we're experiencing another major breakthrough all over again.

Let's be clear: in the software development field, we are all knowledge workers. We don't break a sweat physically to get our work done, we're using our brains.

As outlined in this IBM article, a knowledge worker is a professional who generates value for the organization with their expertise, critical thinking and interpersonal skills. They're often tasked with developing new products or services, problem-solving, or creating strategies and action plans that will drive better business outcomes. Knowledge workers have formal training or significant experience, are skilled communicators and can learn and adapt to a shifting work environment.

As we frequently hear in the news, the supply of developer talent isn't keeping up with the growing demand for new digital services. In respon-

se, developers are becoming early adopters of AI agents and copilots to accelerate and enhance their work.

There's no doubt that this technology is still in its early stages. It's not perfect, and the output from AI can sometimes be completely inaccurate. In addition to that, we still have significant challenges to tackle regarding ethics, bias, privacy, and security. Getting AI right is a journey that still lies ahead of us.

These days, AI is, in many ways, brilliantly stupid, and that's fine. No early technology is perfect.

But, despite the mix of fear and skepticism we hear from many companies and some individuals in LinkedIn posts, AI has been rapidly infiltrating the software development industry, whether we like it or not.

As developers accelerate their work through agile practices, DevOps, and widespread adoption of AI, testing becomes the bottleneck.

In this survey from GitHub on AI's impact on the developer experience, it highlights that "waiting on builds and tests is still a problem. Despite industry-wide investments in DevOps, developers still say the most time-consuming thing they're doing at work besides writing code is waiting on builds and tests. Notably, developers say they spend the same amount of time waiting for builds and tests as they do writing new code".

This is a call to action for those of us in the software testing and quality engineering space. As the ultimate knowledge workers, we should remain open-minded about experimenting with the latest wave of AI tools.

The more we experiment with these new AI tools, the better we can understand their value and limitations, as well as how they can be integrated into our workflow.

To be real, I love getting my work done quicker and better. Like I mentioned before, I switched from handwriting to typewriters and then to word processors. I really appreciate how these changes have helped me out.

In the testing field, much of our work involves routine, procedural, or algorithmic tasks. Trust me, these are the perfect candidates to take advantage of AI tools.

Can a computer do what I do faster and more cheaply? Count me in, so I have more time to focus on creative or strategic tasks.

Or I could use AI to generate a variety of possible testing ideas, so I can refine them with my experience and creative vision. Absolutely, I'm on board!

I don't expect AI to mimic creative human thought processes anytime soon, probably not in my lifetime, but I'm more than happy to take advantage of any leverage it can provide at its current stage.

If it can take care of the happy path and greenfield cases with little input from me (or light review), that would free me up to dive into the tricky corner cases or the ones that really need my experience, creativity, or a collaboration with a subject matter expert (SME). That would definitely save me some time!

At the end of the day, AI should be seen as a tool to augment, not replace, human testers. By automating menial tasks, AI frees us up for meaningful and innovative work.

We don't need to fear AI taking our jobs; we need to be concerned about the people using AI taking our jobs (yes, I know! I've seen plenty of LinkedIn posts where people call this a silly statement, but I still believe it's true).

I believe the key to success lies in mastering AI tools to gain a significant competitive advantage.

To stay relevant, it's essential to embrace these

tools and learn what and how to delegate effectively to AI. Sometimes, certain tasks need to be carried out manually by humans. That's fine, as the goal is not replacement but augmentation.

Before we know it, we'll see the rise of the hybrid tester, QA/QE professionals working in tandem with AI.

The future of work isn't likely to be about humans versus machines, but rather about working together with AI.

I'm glad you made it to the end of the article! I'd like to ask a favor: please share in the comments which AI tools and methods you're using. Feel free to share your success stories as well as any failures you've faced, so we can all learn from our collective knowledge.

Cristiano Caetano
Vice President of Product Management
Katalon

Detailed information in the techL profile: Katalon

SECURITY INSIGHTS

United Innovations

18 SEP, 2025	OT-Security 3:30 - 5 PM ONLINE	
25 SEP, 2025	Post-Quantum Kryptografie 3:30 - 5 PM ONLINE	
02 OCT, 2025	Drivers of Cybersecurity 3:30 - 5 PM ONLINE	
13 NOV, 2025	Security Analytics & Automation 3:30 - 5 PM ONLINE	
27 NOV, 2025	Cloud Security 3:30 - 5 PM ONLINE	

Self-Healing IT: How Pioneerdesk Redefines IT Stability and Efficiency

Imagine a world where IT problems solve themselves — without tickets, without frustration. Pioneerdesk is making this vision a reality with the first self-healing IT platform specifically designed for Windows-based infrastructures.

An article by Marcus Lenczyk, Pioneerdesk

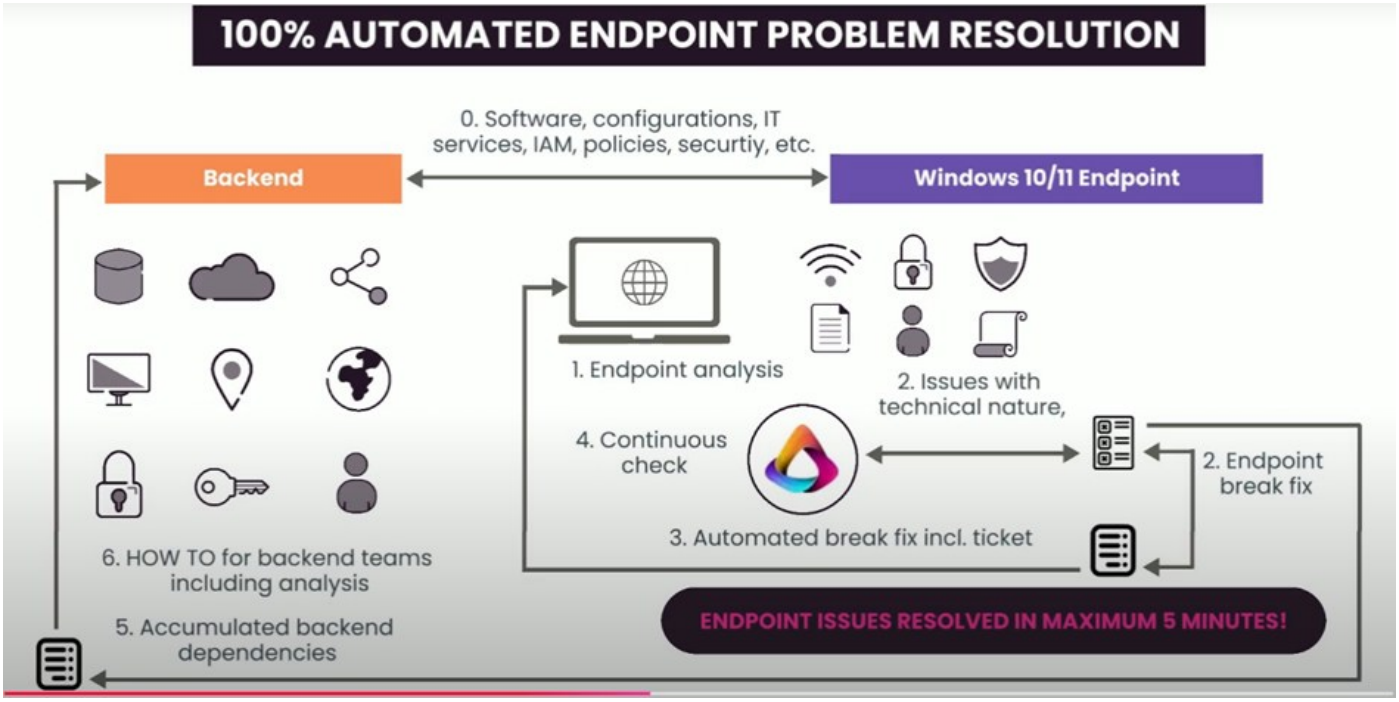


Image: Pioneerdesk GmbH

Founded and developed in Germany, Pioneerdesk revolutionizes IT support by detecting technical errors across all Windows endpoints, providing instant self-repair or precise, scalable fix instructions.

While many companies still fight daily fires with manpower and ticket systems, Pioneerdesk addresses the root cause — transforming reactive IT operations into proactive stability.

Why Self-Healing IT?

Every click that doesn't work, every printer that remains silent, every Outlook crash — costs not just time but damages productivity and morale.

Existing tools flood IT teams with fragmented data but fail to deliver clear, actionable insights. Pioneerdesk closes this gap by combining real-time diagnostics, intelligent pattern recognition, and scalable automation into a seamless self-healing solution.

Concrete Example:

- Before a user even notices that the printer "doesn't work," Pioneerdesk detects a failing driver, repairs it silently — and the document prints without delay.

- Similarly, if critical log events predict an upcoming Outlook crash, Pioneerdesk automatically prevents the failure before it affects the user.

Why Now?

As businesses worldwide face growing IT complexity, talent shortages, and increasing OPEX pressures, the need for a self-healing IT platform becomes existential.

Pioneerdesk already proves that autonomous IT recovery is not science fiction — it's happening today. Companies adopting Pioneerdesk see up to 90% fewer endpoint disruptions and a massive reduction in IT support tickets, often within the first 60 days.

At the IT-Summit Germany, Pioneerdesk proudly showcases how hospitals, SMBs, enterprises, and Managed Service Providers (MSPs) can finally achieve true IT resilience — automatically, scalably, and reliably.

Meet the Author: **Marcus Lenczyk**

CEO & Founder, Pioneerdesk GmbH

8x tech founder, one exit, and 20+ years in enterprise IT automation.

Passionate about turning complexity into clarity and creating software that simply works.

Quick Facts

- Developed and hosted entirely in Germany
- Up to 90% fewer endpoint disruptions
- Automates IT fixes before users even notice problems
- Enterprise-grade security, ready for hospitals & MSPs
- 16€/device/month – with full ROI in under 60 days

Marcus Lenczyk
CEO/CTO
Pioneerdesk GmbH

Mastering Data Quality

In an era where data-driven decisions play a key role in a company's success, high data quality is essential. But which methods and techniques truly help? Do Data Observability and Data Mesh make the difference?

An article by Dr. Jens Bleiholder, OPITZ

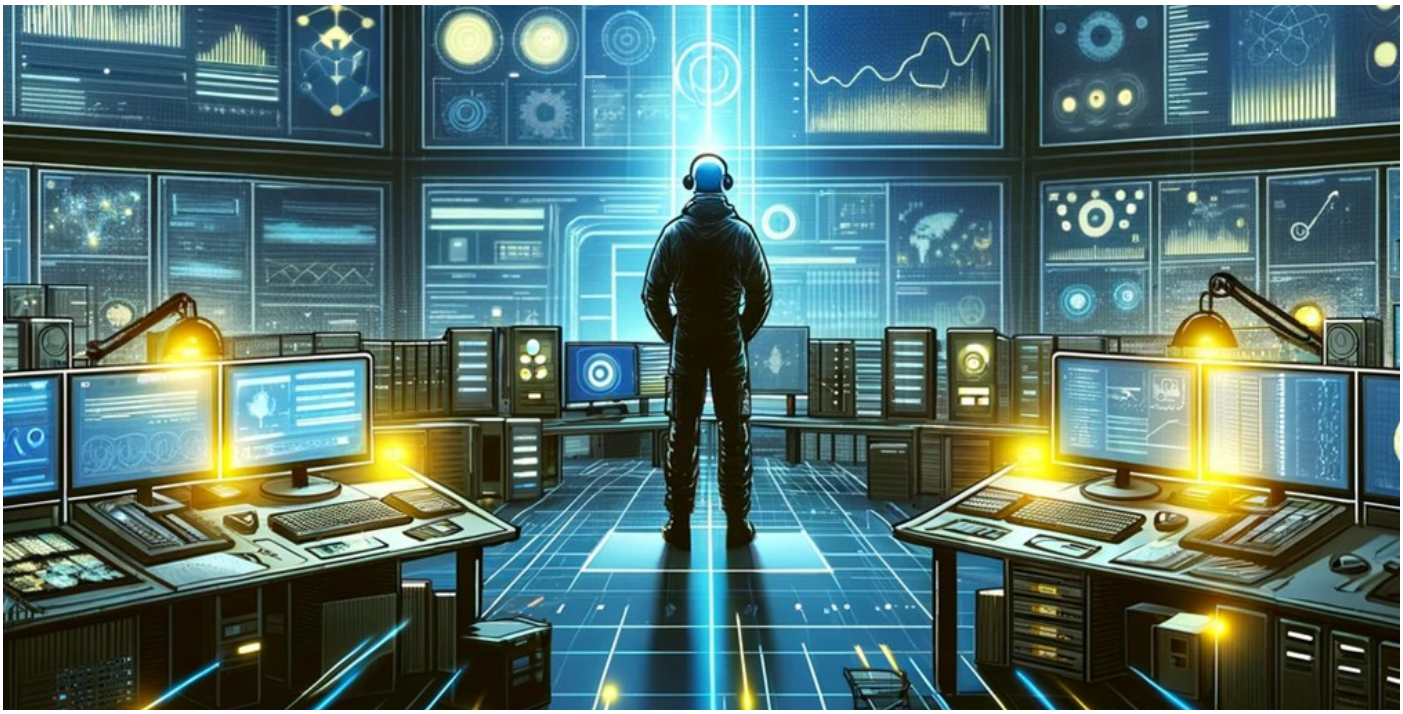


Image: OPITZ CONSULTING Deutschland GmbH, (Dall-E, OpenAI)

Neither organizational concepts like Data Mesh nor technical solutions like Data Observability are silver bullets. But they offer valuable impulses to systematically improve data quality within companies – and to lay the foundation for trustworthy, high-performing AI applications. Time and again, practice shows: good data is often more crucial than good algorithms.

Data Observability – The Technical Foundation for Reliable Data

Data Observability refers to the ability to continuously monitor, analyze, and trace the state of data and its transformations within an organization. The goal is to detect anomalies early, identify root causes of errors, and ensure the integrity of data-driven processes.

It focuses on five key dimensions:

1. **Freshness** – Are the data timely and available at the expected frequency?
2. **Schema** – Does the data structure comply with defined standards and interfaces?
3. **Volume** – Do data volumes significantly deviate from expected values?
4. **Data Quality** – How accurate, complete, consistent, and plausible are the data?
5. **Data Lineage** – Can the origin and processing steps of the data be clearly traced?

Modern ELT tools like dbt (data build tool) provide comprehensive support for Data Observability. They enable the definition of automated tests

for these dimensions – through native functions, community extensions, or custom scripts. These tests can be embedded early in the development of data pipelines and seamlessly integrated into CI/CD processes. The result: continuous, automated monitoring that helps detect and resolve data quality issues as early as possible. There are also specialized Data Observability tools on the market that focus exclusively on monitoring data health and can be used alongside any data processing stack.

Data Mesh – An Organizational Lever for Sustainable Data Quality

While Data Observability enhances technical monitoring, Data Mesh provides an organizational framework for strategically managing data. It targets the scaling of data architectures in large organizations and is based on four core principles:

- **Domain Ownership** – Responsibility for data lies with the business domains. They own and manage their data from source to output.
- **Data as a Product** – Data is treated like a product: it must be high-quality, well-documented, discoverable, and built to serve users' needs.
- **Self-Serve Data Platform** – Teams can easily access and use shared data infrastructure and tools - enabling autonomy and speed.
- **Federated Governance** – A shared set of rules and standards ensures consistency across domains, while allowing decentralized execution.

Especially the principles of *Domain Ownership* and *Data as a Product* have a direct impact on data quality.

Domain Ownership: Business units take responsibility for "their" data – not only technically, but also in terms of content. Their subject-matter expertise ensures data is captured correctly, consistently, and completely. At the same time, data-consuming teams define their quality requirements. Communication between producers and consumers is formalized through so-called *Data Contracts*. Thus, quality is not only ensured through control mechanisms but through clear ownership and collaboration.

Data as a Product: Data is not just made available – it must be useful, valuable, and trustworthy. This requires a shift in thinking: data is treated like a product – with a clear purpose, a defined lifecycle, and concrete quality metrics. For providers, this means more than technical availability – it also involves documentation, testing, and maintenance. This product mindset fundamentally changes the role of data producers and raises the expectations of consumers.

Conclusion

Data Observability and Data Mesh are not miracle cures – but they are powerful levers to improve data quality. What becomes clear: technology matters, but people are the real success factor. Automated testing and monitoring, conscious handling of data products and contracts, and clear accountability are key. Only then can the foundation for long-term, data-driven success be established.

Dr. Jens Bleiholder
Chief Architect Data & Analytics
OPITZ CONSULTING Deutschland GmbH

GenAI successfully integrated into the group

An article by Dr. Gernot Klein, Dataiku

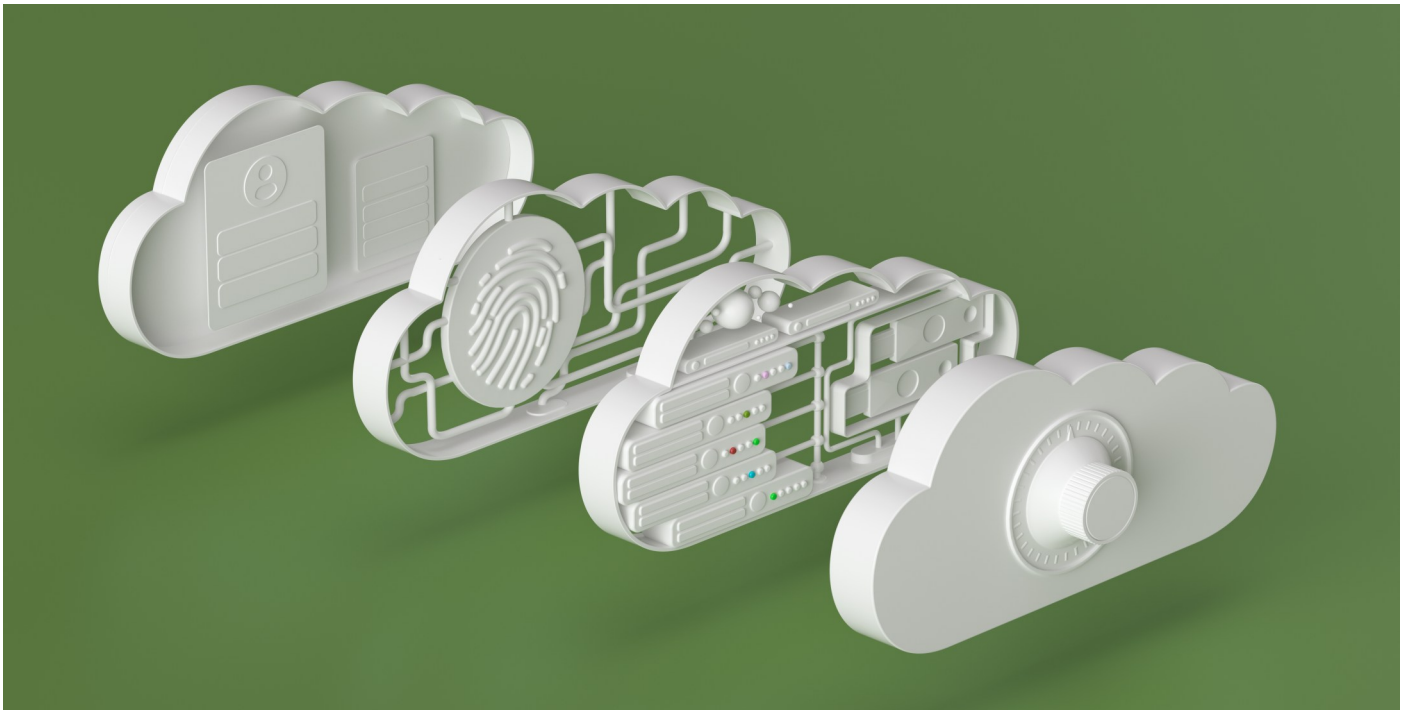


Image: Dataiku GmbH

Hopes are high and expectations as well when it comes to the integration of generative AI (GenAI) and large language models (LLMs) in particular. Companies worldwide see the potential in these technologies to increase their productivity and competitiveness. Despite these high expectations, there is often a gap between what business leaders aspire to achieve and what can actually be implemented at present. A key stumbling block for progress is often an inadequate IT infrastructure, in addition to a lack of clear operational guidelines and processes.

Identifying and overcoming hurdles

In a recent survey of 400 IT executives conducted by Dataiku, 70 per cent of respondents said they use GenAI and LLMs in one way or another. However, GenAI is only routinely integrated into everyday workflows for 20 per cent of respondents. Many companies are still stuck in the unstructured experimentation phase because they lack specialised tools and well-thought-out processes. According to the survey, half the correspondents say that their current data tools and infrastructure do not meet the requirements of GenAI applications. In addition, 43 per cent of respondents report that their current data analysis stack is outdated and does not meet the latest standards. These shortcomings illustrate the discrepancy between ambitious goals and practical feasibility.

For companies that want to take the leap from the experimental phase to the routine use of GenAI and LLMs, it is therefore essential to invest in the necessary data and IT infrastructure.

One of the main prerequisites for value-adding AI applications has not changed: well-curated and thus trustworthy data that is easily available

throughout the company. According to the Dataiku survey, 45 per cent of respondents report that data quality is a critical issue, while 27 per cent call out a lack of access to data, slowing down the development of AI-based applications. To make matters worse, companies now not only have to worry about the curation and accessibility of their structured data, but also about their unstructured data, from emails and product instructions to customer communication, which they have to prepare and make available for AI applications. This is the only way to adapt the powerful LLMs, which are usually trained with generic data, for company-specific use cases.

Creating room for development

Another crucial aspect for the profitable use of GenAI in companies is an effective development process that allows ideas for GenAI applications to be quickly converted into so-called proof of concepts (PoCs) and, if these have proven to be value generating, to then be smoothly operationalised, i.e. integrated into everyday business processes as an integral part. To do this, companies with diverse data engineering and data science teams, ideally need to set up standardised development environments. Without such development environments, which allow different teams to work together effectively and share results with all stakeholders, a fast and smooth development or iterative adaptation of AI and GenAI applications is often difficult, leading to only sporadic adaptations to changing business conditions and applications quickly losing their original added value. The use of an end-to-end platform like Dataiku, provides such a development environment, covers the entire development cycle and enables the rapid development of GenAI applications, as well as their maintenance and continuous monitoring and management.

An important feature of these standardised development environments is their interoperability. Not only with a wide range of (cloud) databases to ensure seamless access to all company data, but in particular for GenAI applications the ability to work with more than one LLM (provider). This makes it possible to 'decouple' the value-adding application facing the end user from the LLM used. In a field that is developing as rapidly as GenAI research, this is essential to ensure that developed GenAI solutions that are routinely used in the company can continue to be operated even if the underlying LLM needs to be replaced.

Compliance is imperative from the outset

Another increasingly important feature is the integration of a comprehensive 'governance framework', i.e. the option of making both the development and the deployment of GenAI applications in the company as transparent as possible, thereby ensuring that they are used in accordance with company rules and regulations such as the EU AI Act. Here, it is crucial to have the governance requirements in mind from the outset, i.e. as early as the planning of GenAI applications, and to implement them directly during development. Trying to 'catch up' at a later stage is rarely possible or efficient. In the future, more and more tools or agents will use or connect to GenAI models. Companies that manage to adapt their IT systems and processes accordingly will be able to leverage the advantages of GenAI more effectively and gain a decisive competitive advantage. Overcoming these challenges requires both technological investments and strategic foresight to turn the ambitious goals of executives into tangible successes.

Dr. Gernot Klein
Field Chief Data Officer
for Central and Northern
Europe
Dataiku GmbH

From guesswork to explainable insights: Why GenAI needs Knowledge Graphs

An article by Irina Schmidt, metaphacts

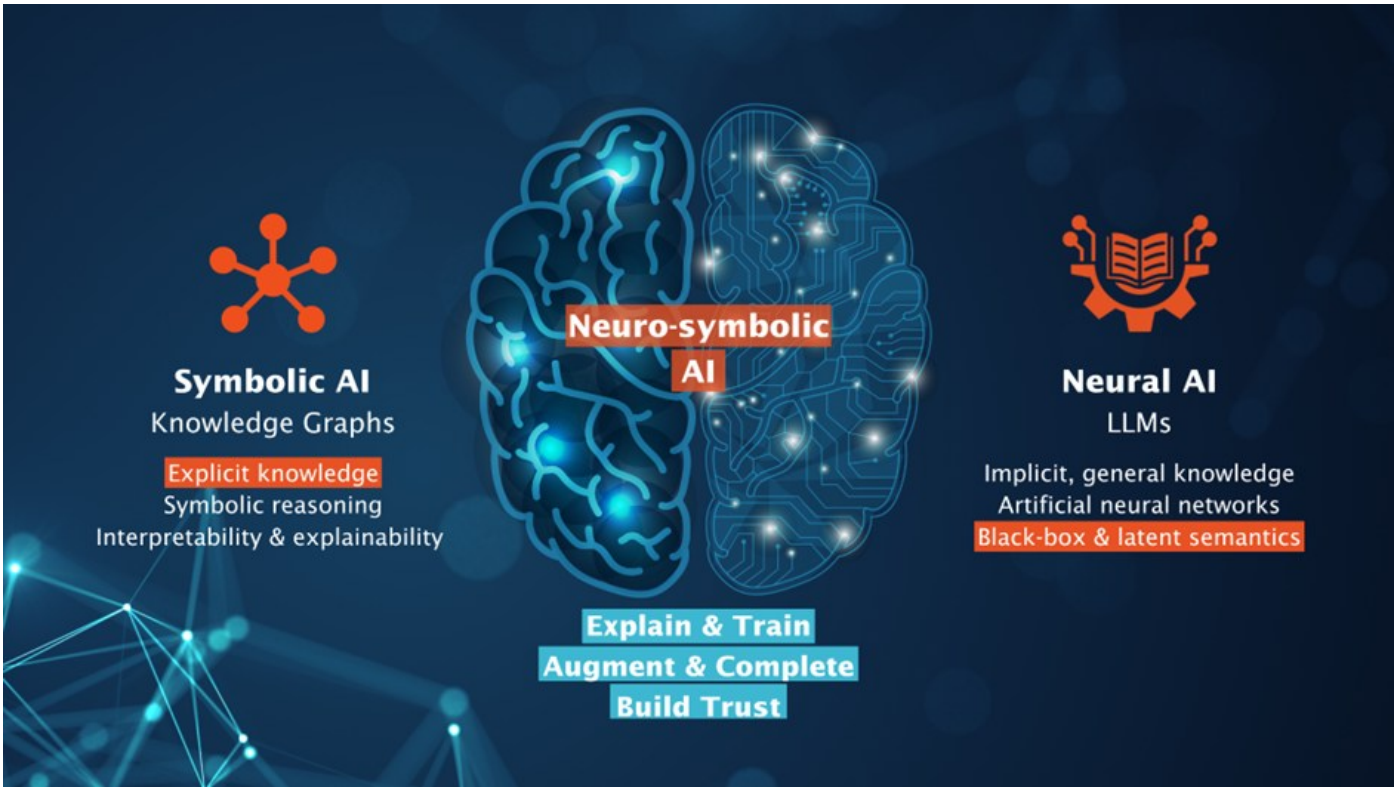


Image: metaphacts GmbH

Generative AI is revolutionizing how organizations interact with data and make decisions. But beneath the surface of impressive language models and productivity gains lies a pressing concern: can we trust AI-generated outputs in high-stakes business environments?

The answer lies in semantics, in practices that add meaning to enterprise data—and in building knowledge-driven, agentic AI solutions that move beyond surface-level understanding to deliver contextual, traceable and trustworthy insights.

Why LLMs alone aren't enough

Large Language Models (LLMs) have rapidly become go-to tools for content creation and data exploration. Yet, they remain trained on general-purpose internet data, often lack transparency and are prone to hallucinations. In enterprise settings, this can lead to misleading results, regulatory risks and loss of control over sensitive data.

LLMs are powerful but operate in a black box: their outputs are shaped by implicit patterns and statistical approximations rather than explicit business logic. Without access to enterprise-specific semantics, which adds essential business context to data, they fall short in delivering meaningful insights that are explainable, auditable and aligned with internal knowledge and expertise.

Bridging the gap with Knowledge Graphs

Knowledge graphs bridge this gap by introducing explicit, structured knowledge into AI systems. They embed domain expertise, business rules and contextual meaning into a machine-readable format, making it possible for AI to reason, explain and adapt.

When fused with LLMs in a neuro-symbolic approach, knowledge graphs act as a semantic foundation—anchoring AI in factual, verifiable content while enhancing its interpretability. This results in AI agents that are not only powerful, but accountable and aligned with enterprise goals.

Building knowledge-driven & business-aware AI Agents

To unlock GenAI's full value, organizations must shift from generic assistants to agentic AI—autonomous systems that detect user intent, orchestrate tasks and make decisions. But autonomy without business context is just rudimentary automation at scale.

Knowledge-driven AI agents offer a better path forward. They combine:

- Semantic models that ground responses in an enterprise's unique context and domain knowledge
- Transparency that enables users to trace decisions back to source facts
- Adaptability to evolving data landscapes, without costly retraining
- Privacy controls and compliance guardrails to meet regulatory standards

From data silos to strategic decisions

The key to realizing these benefits is an AI platform that integrates knowledge, language and logic. At metaphacts, we've spent the last decade helping organizations build semantic knowledge graphs. Now we're taking that vision further.

Coming in early July 2025, **metis** is our new AI platform that transforms disconnected enterprise data into explainable facts to guide goal-oriented AI agents. With metis, users can:

- Design and deploy custom agents that users can interact with via a conversational interface
- Ground AI responses in a semantic layer for accuracy and trust
- Control and audit how enterprise data is used
- Combine tools like summarization, entity linking and query execution—all scoped by business-specific semantics

The future is knowledge-driven

As GenAI reshapes how we work, the difference between success and failure will hinge on context, trust and control. Knowledge graphs make that possible. They don't replace LLMs—they elevate them.

It's time to move from generic assistants to business-aware AI agents that understand not just language, but your business. That's the promise of knowledge-driven agentic AI—and it's what powers metis.

Irina Schmidt
CMO
metaphacts GmbH

Evolution of AI Agents

How smart are your automation systems? This technological revolution spans all industries, requiring collaboration between AI developers, process engineers, and executive leadership to successfully implement truly intelligent systems.

An article by Ruben Schilling, Roboyo

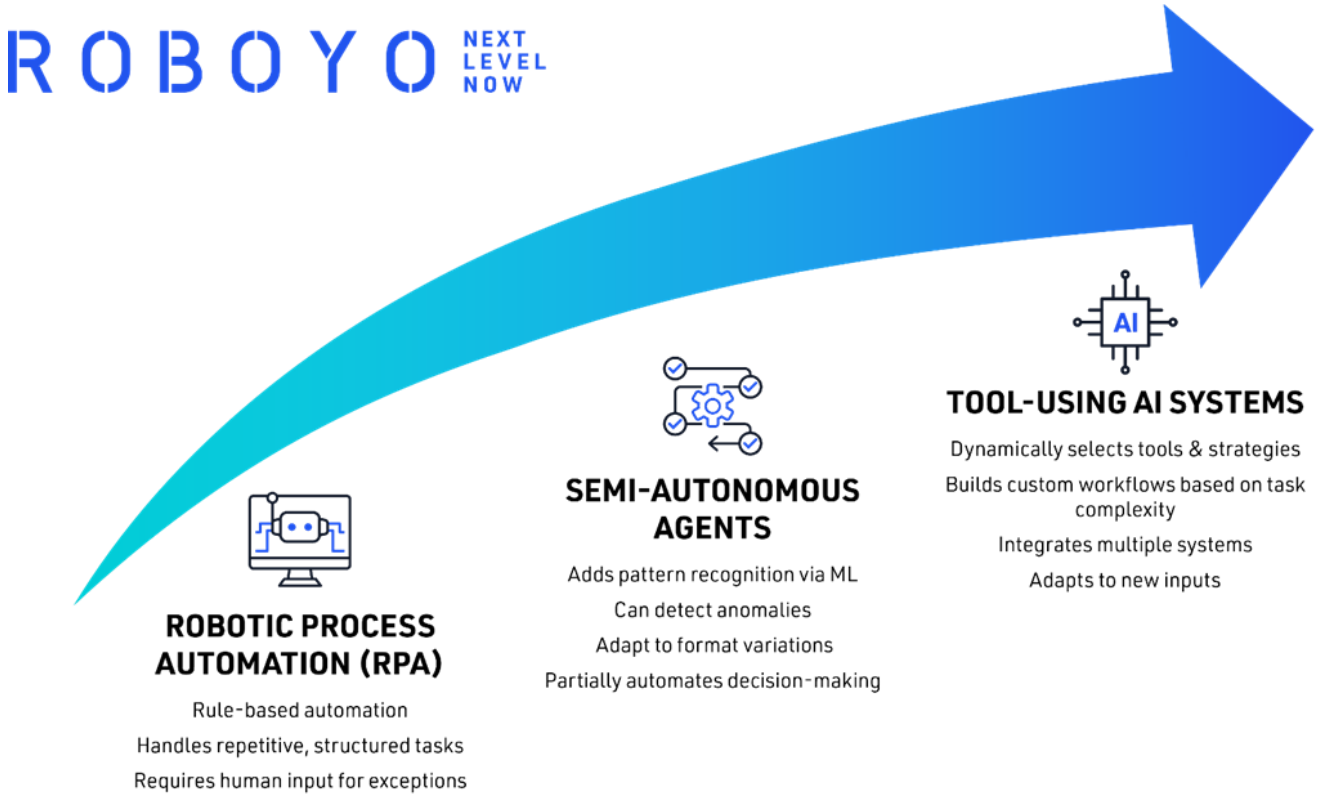


Image: Roboyo GmbH

The progression of artificial intelligence agent technologies has transformed business processes across industries. Using invoice processing as our illustrative example, we can visualize how these technologies have evolved from basic automation to sophisticated systems that independently make decisions and select appropriate tools.

Stage 1: Robotic Process Automation (RPA)

The journey began with RPA, where rule-based systems automated repetitive tasks. These implementations extracted information from standardized invoice forms, verified vendor details, and performed calculations according to fixed rules. While effective for standardized invoices, many still required human intervention due to the system's inability to handle variations in formats or discrepancies between invoices and purchase orders.

Stage 2: Semi-Autonomous Agents

With machine learning advancements, organizations progressed to systems with basic decision-making capabilities. These semi-autonomous

agents identified patterns in historical data, detected anomalies that might indicate duplicate or fraudulent invoices, and analyzed document layouts to extract data regardless of format variations.

In invoice processing, these systems transformed operations by matching invoices to purchase orders even with partial information, categorizing expenses automatically, and determining appropriate approval workflows based on amount thresholds. This enabled straightforward invoices to be processed in minutes rather than hours.

Despite these advancements, the systems remained constrained by their narrow domains. They handled variations within predefined scenarios but struggled with new situations, still requiring human guidance for unusual invoice formats or exceptions that didn't fit established patterns.

Stage 3: Tool-Using AI Systems

The current frontier involves AI systems that actively select and utilize different tools based on specific requirements. This represents a fundamental shift from following predefined processes to dynamically assembling custom approaches for each task.

Tool-using AI systems select appropriate analysis methods based on specific characteristics. They access specialized software tools and databases as needed, customizing workflows based on complexity and relationships. These systems determine which tasks require human expertise and which can be processed automatically, continuously optimizing their approaches based on outcomes.

In invoice processing, these intelligent systems transform the experience by selecting specific data extraction tools based on document format and applying different matching algorithms depending on the relationship complexity. For straightforward invoices, they employ direct three-way matching, while for complex cases, they analyze contract terms and historical patterns.

What makes tool-using AI revolutionary is its ability to orchestrate complex processes dynamically. Rather than following predetermined workflows, these systems assemble custom approaches from a diverse toolkit based on each case's unique characteristics, determining the optimal processing path with greater consistency and capacity than traditional methods.

Despite these advances, human expertise remains essential for complex situations. The most effective implementations create a partnership between AI and human experts – leveraging technology for efficiency while maintaining human judgment where it adds the most value.

The foundation established by these tool-using systems will enable even more advanced capabilities in the future, including AI that can modify existing tools or create new ones. This evolution demonstrates the transformative potential of AI agent technologies in reshaping business processes for greater efficiency, accuracy, and control.

Ruben Schilling
Manager Intelligent Automation Engineering
Roboyo GmbH

Detailed information in the techL profile: Roboyo GmbH

Harnessing AI in Banking: Between Automation, Regulation and Strategic Value Creation

Artificial Intelligence is changing the banking landscape. What are the implications for customers, bankers and regulators?

An article by Prof. Dr. Alexander Schroff and Zaman Kakhki, Publicis Sapient

Banks globally are redefining their operations by embedding AI into their core functions. AI is not just a back-end utility, it is a transformative force that can enhance efficiency, elevate customer engagement, and reshape compliance frameworks.

Publicis Sapient's Global Banking Benchmark Study signals a clear shift from basic digitization to embracing advanced AI capabilities. Instead of merely improving existing workflows, banks are integrating AI into their business models to automate routine tasks and drive data-driven decision-making. This integration directly impacts customer experiences and overall efficiency, establishing AI as an ingrained protocol rather than a supplementary tool.

Smart Automation with Human Oversight

The partnership between Deutsche Bank and Publicis Sapient exemplifies this shift, focusing on transforming and accelerating the adoption of generative AI for innovation in business models and revenue streams. AI streamlines operations, reduces manual labor, and increases productivity.

Yet, human oversight remains vital to ensure that AI's numerical and evaluative outputs align with complex decision-making and market interpretations. Banks thus invest in harmonizing AI outputs with human insights.

Accelerating Legacy System Modernization

To further bolster these efficiencies, banks are leveraging AI platforms like Sapients Slingshot to accelerate the modernization of legacy systems and the software development lifecycle (SDLC). These platforms enable banks to streamline code updates and integrations, significantly reducing development time. By automating repetitive tasks in the SDLC and offering intelligent insights, they help in overhauling outdated systems efficiently. This allows banks to remain competitive and responsive to fast-paced market needs.

Navigating Compliance and Regulation

While the integration of AI can significantly enhance operational efficiency through smart automation, it also requires ensuring compliance and adherence to regulatory standards. As banks expand AI adoption, they must equally prioritize the establishment of frameworks that uphold security and privacy. This presents both challenges and opportunities for developing AI systems. Anonymization for example is vital when managing personalized services to mitigate risks and build customer trust - essential elements to enhancing customer interactions.

Enhancing Customer Experience

AI revolutionizes customer interactions by analyzing deep data patterns to predict client needs.

Image::Publicis Sapient

By analyzing transaction histories and engagement patterns for customer segmentation and service customization, banking can be transformed into a personalized experience. To enhance service quality and increase operational efficiencies, banks need to provide robust data management and comply with relevant data regulations (e.g. EU AI Act).

Laying the Foundation for AI Innovation

A robust data culture is essential for sustainable AI innovation. Banks are investing in data infrastructures, enabling seamless data flow and facilitating structured data availability. This investment supports continuous innovation and aligns analytics teams with future technological developments. It lays the groundwork for technological alignment and enhancements.

An effective AI strategy encompasses more than technology; it requires strategic alignment across the organization. Leaders are adapting by emphasizing data literacy and ethical standards. Progressive banks view regulation as a framework for compliance, testing systems, using it to adapt systems resiliently and unlock new potentials in operational capabilities. Such an environment turns AI projects from experiments into organization-wide strategies with tangible results.

A Catalyst for Enterprise-wide Change

AI fosters excellence in banking by merging machine accuracy and efficiency with human insight. As banks continue to refine their AI strategies, they focus on enhancing customer trust and satisfaction while remaining agile in a rapidly evolving landscape. By constructing ethical, human-centric technologies, banks aspire to redefine the banking experience through precision, speed, innovation, empathy, and responsibility.

Prof. Dr. Alexander Schroff
Industry Lead
Financial Services
Publicis Sapient

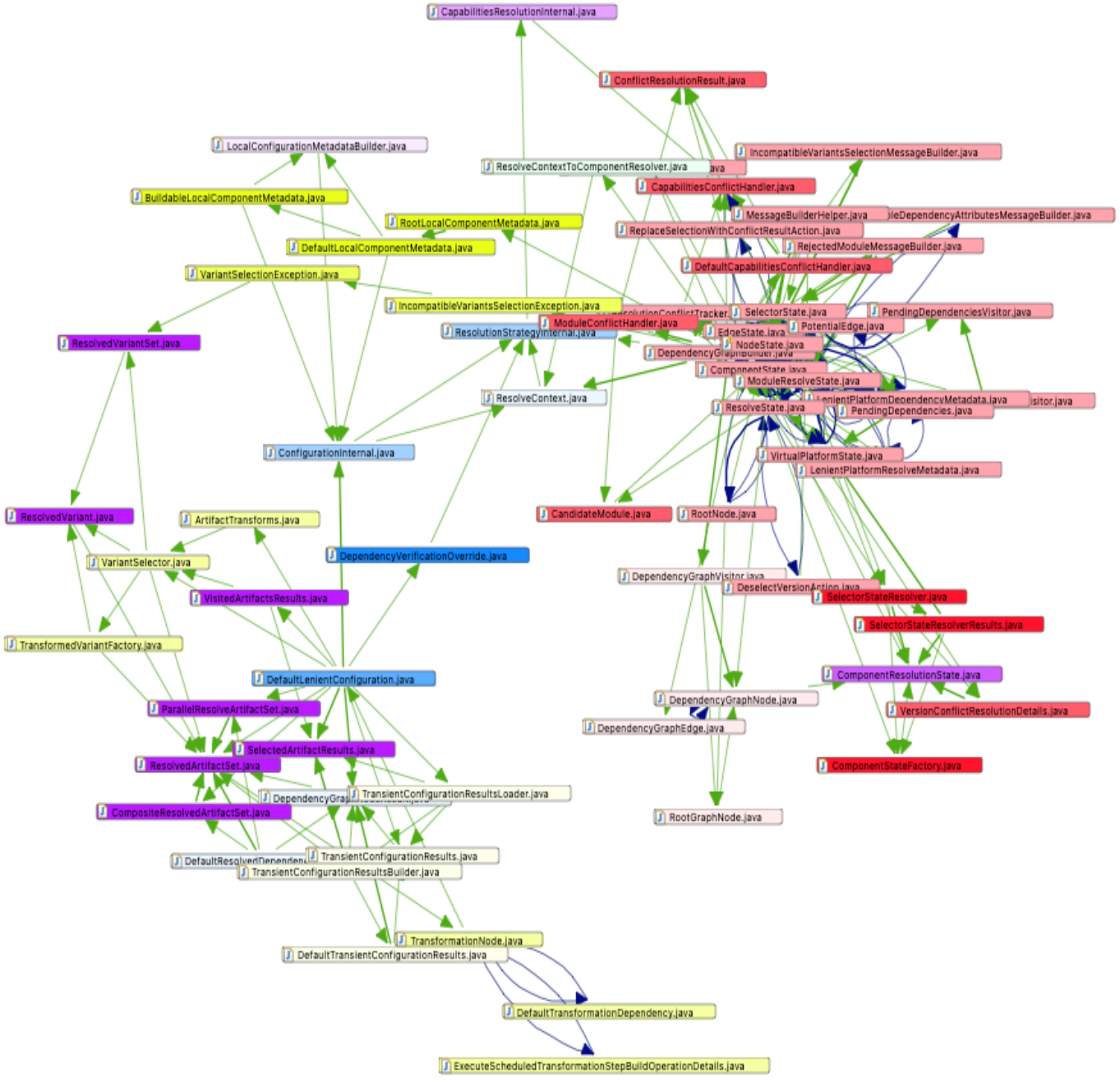
Zaman Kakhki
Manager
Financial Services
Publicis Sapient

Detailed information in the techL profile:
Publicis Sapient

Code Cancer is Costing Billions

You probably never heard about “Code Cancer”, but this term would be an adequate description for some key issues most non-trivial software systems are suffering from. Chances are that your own organization is affected by it right now. In this article I will describe what I mean by “Code Cancer” and offer ideas how to mitigate this problem.

An article by Alexander von Zitzewitz, hello2morrow GmbH



Medium stage code cancer rendered by Sonargraph-Architect

Image credits: hello2morrow GmbH

The screenshot above shows a dependency diagram from the well-known open-source project "Gradle", which is written in Java. Gradle is an advanced tool for building software systems. What you see a cyclic dependency between 69 different Java files, i.e. by following the links you can reach each of the 69 files from any other and come back a different way. We call this a "cycle group" of 69 elements. The different colors mark the different parent packages for the files. This form of coupling creates some real issues:

- It becomes impossible to re-use any of the 69 classes in the cycle group separately from the rest.
- You can test none of those 69 classes in isolation, which makes testing a lot harder.
- Code comprehension becomes much more difficult, because it also becomes difficult to understand any single class without the other 68 ones. This is especially bad, since developers already spend most of their time with reading code.
- Security vulnerabilities are harder to detect in this code jungle.

By doing a lot of research and assessments of complex systems I can confirm that once those cycle groups reach a certain size, they will only get worse over time, hence the use of the term "code cancer". The cycle groups can be seen as tumors, that will grow over time. For example, in Apache Cassandra version 1.0 there was a cycle group with 296 elements. In version 4.1 this tumor has grown to almost 1,600 elements. This is what I would call late-stage code-cancer. To decouple a cycle group as large as this you probably need more time than trying to rewrite the software from scratch.

CISQ came out with a report that estimated the cost of poor software quality for 2022 in the U.S. alone to be 2.41 trillion USD, a whopping 10% of GDP. I suspect that code cancer is a major contributor to this figure. (https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2022-report/).
What we observe here is the structural erosion of the code base, which also could be described as deteriorating architectural cohesion. The reasons for that are plentiful. Most importantly most organizations do not work with enforceable architectural models. If there is an architecture, it is communicated either verbally or over some outdated documents. A mechanism to verify that the code is reflecting the architecture is usually missing. That means developers are for the most part unaware of issues caused by undesirable dependencies and only feel the pain once the code tumors have reached acritical size. By that time, it is already too late to fix the problem in a cost-effective way.

The best way to address this problem is the use of tools that can detect those cycle groups and allow the definition of enforceable architectural boundaries. Two simple rules that can be enforced automatically will guarantee that your systems never suffer from a severe case of code-cancer:

- Never allow cycle groups with more than 5 elements. This rule applies to source files, but also for larger elements like packages or namespaces. When looking at dependencies between packages / namespaces it is best to totally avoid cyclic dependencies. On the source file level certain design patterns are probe to cycles, but as long as the cycles stay small this is not a big issue.
- If you want to walk the extra mile towards excellence you also need to define an enforceable (with tool-support) architectural model.

Both of those rules can easily be enforced in the CI build suing our Sonargraph tool family. For the architectural model we designed a domain specific language which could be described as UML component diagrams in text form. Sonargraph is used by 100's of medium to large sized businesses mainly in Europe, but also in the U.S. and Asia. Many of our customers have been using it for more than 10 years and achieved significant improvements in developer productivity and overall code quality.

Alexander von Zitzewitz
Co-founder and
managing director
CEO of the US subsidiary
hello2morrow GmbH

Detailed information in the techL profile:
hello2morrow

AI Incidents are Expensive - Why Companies are Turning to AI Risk Management & Testing Tools

When AI systems fail or produce discriminatory outcomes, the consequences reach far beyond technical errors. Calvin Risk is dedicated to proactively managing these risks - before they have the chance to emerge.

An article by Julian Riebartsch, Calvin Risk

Image: © Calvin Risk AG 2025

Predictive AI. RAG. GenAI. AI Agents. The world has witnessed a lift-off in AI adoption over the past 3 years, and only now are we starting to see its full impact, both good and bad. While customer service models are showing significant increases in client happiness and efficiency, AI incidents and 'hallucinations' are becoming a reality for many enterprises and is particularly heightened for those who have not yet prepared AI Risk Management and Governance best practices. With that said, how do we move from 'reactive' to 'ready'?

Across the board, industries are implementing AI, especially GenAI systems, at lightning speeds. For example, GenAI systems are used in a variety of use cases, whether for general customer engagement, to technical processes like claims handling for insurers or quality control report summarization for manufacturers. However, such models are far from perfect; these risks range from technical failures and poor performance to ethical concerns, regulatory pressure, and reputational damages. The stakes are high: incidents can disrupt internal processes, lead to

fines, and harm the company's public image. That's why strong, proactive governance is no longer optional.

So, how can companies tackle the operational risks that come with AI and build governance systems strong enough to manage them? There are two actions a company should take:

1. Automated Testing

While pre-deployment testing is now standard practice, current approaches remain manual and subjective. This limits the ability to detect AI hallucinations, bias, and vulnerabilities, and makes it particularly difficult to compare model versions over time. Testing cycles are also inefficient, often taking days to complete.

Calvin streamlines this process with structured, installable tests that evaluate key dimensions such as toxicity, jailbreaks, and context relevance - all in a matter of hours.

2. AI Governance Digitalization

Today, many organizations rely on scattered Excel files to track model inventories, associated policies, and risk exposures. These files are often outdated, lack transparency, and offer little support for strategic oversight.

Purpose-built AI governance tools like Calvin replace this with a centralized system for model and use case management - enabling full traceability, evidence tracking, and a comprehensive view of risk. Moreover, Calvin's configurable questionnaires help guide use case owners through automated, objective risk assessments aligned with the company's operational risk framework. This helps prevent non-AI risk experts from generating arbitrary risk profiles without guidance.

Staying competitive increasingly depends on the *strategic* use of AI, making AI risk management a priority at board level. Calvin Risk helps close this gap by enabling automated testing across key dimensions - quality, fairness, robustness, explainability, and safety - while also digitizing governance and risk frameworks for greater efficiency and transparency.

Our platform offers a centralized model inventory, automated quality and risk assessments, and economic risk analysis. Our methods are both scientifically rigorous and aligned with the real-world needs of our clients, positioning us at the forefront of this emerging industry. With Calvin, organizations can not only quantify model quality and risk but also embed qualitative assessments and governance processes into their workflows. Nothing else combines these essential elements so effectively in one platform.

About Calvin

Calvin Risk is a standardized, automated AI Risk Management software. It enables users to systematically evaluate AI systems via API endpoints or model uploads, automatically create ground truth test data using context information, and leverage a library of 50+ metrics to assess system quality across bias, hallucinations, and attacks. Built on research from ETH Zurich with risk dimensions aligned with NIST and EU AI Act standards, Calvin Risk ensures rigorous, reliable risk assessment.

Julian Riebartsch
CEO & Co-founder
Calvin Risk AG

Detailed information in the techL profile:
Calvin Risk AG

Quality Assurance of AI Applications: Between Hope and Reality

An article by Dr. Niels Heller and Bastian Knerr, QualityMinds

A Small Problem to Get Started

Born out of a deep-rooted focus on testing and quality assurance, our company has grown into a multifaceted tech partner, expanding into software development, AI & machine learning, consulting, and data infrastructure. That breadth of expertise is one of our strengths—but it also presents a challenge.

We have many experts in many fields. That's great! But there's a catch: Who can do what, with what formal qualifications? No one has the full overview. As soon as business opportunity reaches our system, a kind of mini matching algorithm has to kick into gear. Speed is essential here.

Verifying such requirements by hand is expensive and time consuming, hence automation seems like an obvious solution. Large language models (LLMs) appear as ideal candidates for the task: they can analyze job or project descriptions which might suit our business and match them with qualifications from HR records. After all, LLMs are trained to recognize patterns and handle various input formats. Sounds promising—but does it work in real-life application?

LLMs as the Digital Swiss Army Knife?

This idea applies to many digitization problems. Traditional automation, i.e. programming, only works if everyone sticks to pre-defined and structured data formats – which is rarely the case. Recently, I was thrilled to find that a public provider offered data in XML format—until I realized that 90% of the relevant information was hidden in a free-text field, containing, again, unstructured information.

Language models are seen as beacons of hope. Their architecture allows for various applications including information extraction, rephrasing, entity detection, etc.

The Challenges

The temptation to use LLMs, even for benign tasks is strong. Yet, there are some major challenges to this use.

First: LLMs only process tokens—strings of characters without implicit meaning. That creates vulnerabilities: a manipulated document can silently reprogram the model—a problem known as *prompt injection*. Unlike traditional SQL injections, there's no reliable fix for this yet.[citation prompt injection]

Second: LLMs are statistical systems. They generate plausible-sounding answers, but those can be wrong. Self-correction mechanisms only help to a limited extent because the models lack real understanding of **AI Quality Assurance: A Structured Approach**

In our work, we've developed two methods that are now part of our standard toolkit for AI applications:

AI Risk Storming: Stakeholders (developers, clients, users) jointly discuss the core functions of an application and evaluate risks and countermeasures. What quality metrics are critical? What threats could endanger them?

HACCE Approach: This method uses formal critiques to uncover weaknesses. These critiques arise from analyzing validation data. The motto: A mistake is only a problem if no one knows about it.

But every method needs to applied in the correct context and in order to provide guidance for our clients, we introduced a new “AI Testing Pyramid” which is derived from the classic software testing pyramid. We believe firmly that AI Quality Assurance, partly by borrowing and adapting concepts from traditional software testing, will deliver much needed efficiency and accuracy to this field.

Overall, quality assurance for AI isn’t an afterthought—it must be integrated from the very beginning. In Software Testing “Shift Left” is a core principle which will be needed even more in the era of AI, as data is the main driver of quality in LLM systems. Blind trust in an LLM often results in outputs that sound good but are unreliable. Structured testing methods, data governance, robust metrics, and a critical eye are essential to making AI deployment both meaningful and safe.

errors.

Third: Implementation concerns. These AI models consume enormous amounts of energy. And there's the risk of vendor lock-in: relying too heavily on a single provider makes one dependent on their (opaque) technology.

Quality Assurance for AI: What Can Be Done?

Language models are often said to have creative potential. If we consider creativity as the ability to come up with *valuable* new ideas, we see the caveat of this technology. LLMs can certainly generate new ideas in abundance—but the evaluation needs to be provided by another system.

The standard response from the AI industry has been to scale up the model sizes in hopes of training models that have a higher chance of producing more valuable ideas. But that doesn’t scale indefinitely—eventually, you run out of training material. And despite of these efforts, social media is not shy in publicizing the latest AI-fails, such as lawyers trying to use hallucinated precedence to make their case.

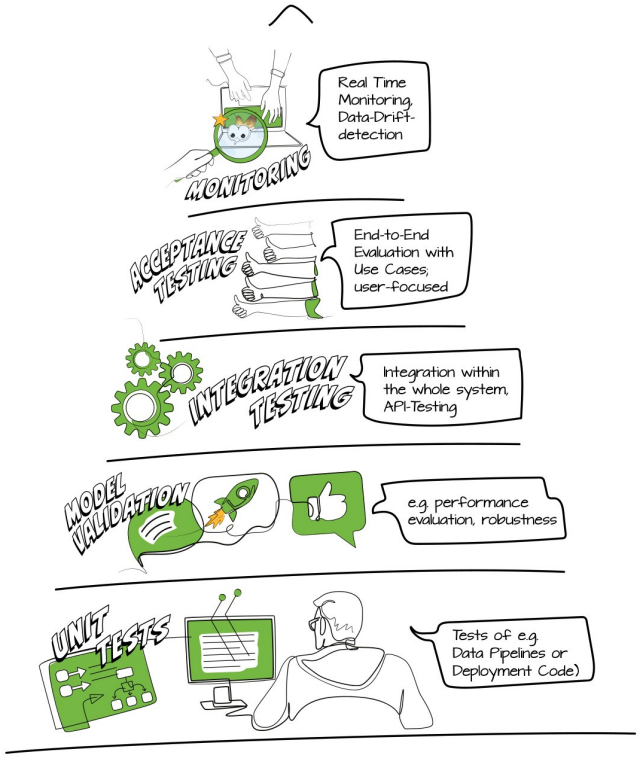


Image: QualityMinds GmbH

Can LLM-outputs even be evaluated programmatically? Statistical metrics like BERTScore can at least measure semantic similarity, which could have at least helped that lawyer (seeing a low semantic similarity to any documented case might have sparked suspicion).

Similar problems apply to the initial problem of request assessment: exact terms are often expected here. One company was looking for someone to "write test cases." We offered an expert who "creates test cases." Result: automatic rejection. A small detail that can come at a high cost.

Dr. Niels Heller
Tech Lead AI
QualityMinds

Bastian Knerr
Teamlead Testing
QualityMinds

United Innovations

Release 2025 - IT Summit

www.united-innovations.eu