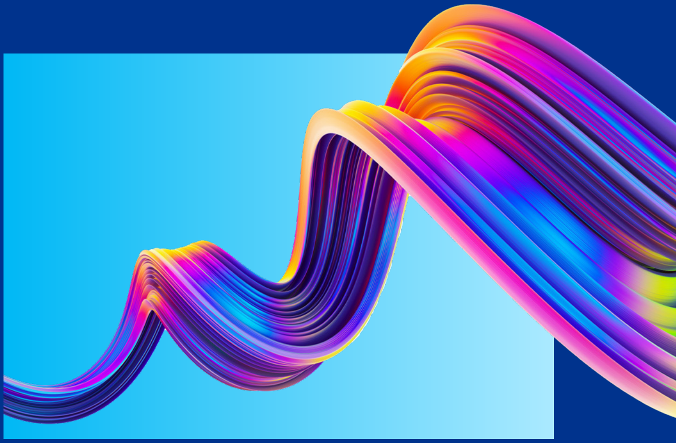
The lowdown on low code

KPMG Technology Risk Modernization Center of Excellence



Organizations are embracing low-code platforms to speed up their digital transformation journey—enabling them to innovate, manage cost, and react to business challenges and opportunities with unprecedented speed.

Low-code automation has the potential to accelerate business outcomes, but organizations should understand ways to manage potential risks along the way.

The rise of low code

Even as digital technologies change our world at a breathtaking pace, some companies are finding their own digital strategy stuck in low gear. They struggle to amplify their work, incorporate it into their legacy processes and information systems, and orchestrate their actions efficiently across the organization. The following challenges have impeded many businesses from achieving their digital transformation goals, too often resulting in a siloed application ecosystem with marginal business use and no measurable return on investment:

- Market demands: Rapidly changing business conditions and market demands have driven the need to speed up digital transformation initiatives and business process optimization.
- Communication: There exists a large gap between business user expectations and the end product.
- Legacy processes: Organizations are constantly customizing legacy processes to meet changing demands.
- Talent scarcity: Overwhelming backlog of application enhancement projects coupled with the shortage of software developers.
- Ambitious goals: Overambitious goals and unrealistic release plans cripple quality development activities.

Low-code technology offers a better way forward

- Low-code is arguably one of the most disruptive technologies to hit the enterprise since the cloud. Through a simple graphical interface, prebuilt functions, and drag-and-drop simplicity instead of traditional manual programming, it allows you to create automated workflows and powerful applications.
- With low-code platforms democratizing technology, the concept of citizen developers—business domain professionals and end users with little to no software development experience—is growing in popularity. Businesses are now accelerating modernization and developing solutions that were previously highly dependent on IT resources. In turn, this enhances innovation, reduces costs, and increases the overall competitiveness of an organization.
- Traditionally, applications developed in programing languages such as Java or .NET offer very limited customization and flexibility. Moreover, organizations must hire the right talent to leverage it. Enterprise solutions like Oracle and Workday are off-the-shelf applications making them even more inflexible. This is where low-code applications come into play. Low-code platforms like Power App, Appian, and ServiceNow make it easy to tap into the backend of your legacy systems, customize, and deploy faster to drive automation and provide enterprises with the agility required to thrive in today's digital-now, digital-first environment.

Potential benefits of low-code automation

Low-code development has become a powerful enabler of automation and innovation that is lighting up opportunities beyond the obvious. It puts more problem-solving capabilities into the hands of non-IT professionals while enabling employees with varying degrees of experience to swiftly produce scalable business applications in response to shifting business demands.

- Decrease in "translation" problems between business and IT; low-code platforms empower citizen developers to build applications that fit their needs without high reliance on IT
- Reduced pressure on an already stretched IT department, allowing it to focus on bigger transformation projects
- Low-code platforms have prebuilt, reusable functions that allow a reduction in the cost of application development
- Rapid development of new business applications, enabling companies to quickly adapt to the shifting markets with agility.

By 2026, developers outside of formal IT departments will account for at least 80% of the user base for low-code development tools, up from 60% in 2021. In addition, the market for low-code development technologies is projected to grow to $44.5 billion by 2026 at a compound annual growth rate of 19%.* Therefore, it is critical for organizations to empower people—citizen developers—to be able to help organizations implement automation faster and enhance the client experience.

Industry-specific use cases

Agility and velocity are important factors in software development operations, but they're especially critical in the following industries that need to scale their operations or quickly pivot against broader market changes:

Healthcare: Low-code platforms allowed patients to access and share information more easily or make appointments within an online environment that is already compliant with certain regulatory frameworks such as HIPAA out-of-the-box. The IT team can set up the platform, enabling citizen developers to build customer-facing apps that integrate with the enterprise systems on the backend.

Financial services: Using low-code application, a financial services firm streamlines workflow for creating, reviewing, and reporting risk data across departments while adhering to regulations, which was able to bring together different data sources of legacy applications into a standardized platform. The application is easily customizable by employees and gives insight in process performances and task distribution.

Retail: A low-code application was developed for customer appointments, meeting facilitation, and dashboarding of sales data to gain insights into the effectiveness of the sales process across the organization and build maps for internal usage. Another app was developed for master data management to monitor master data changes and additions along with approval requests.

- Process understanding, comprehensive data, and compliance requirements are key factors in a successful 3LoD model. Low-code or no-code development provides approaches to excel in each of the three key lines of defense:

  Operational management: HR citizen developers can build tools to identify knowledge gaps and allocate relevant training sessions. They can also create a user-friendly database with access to all internal and external compliance requirements while connecting with HR information to monitor and assess risks.

  Risk management (RM): RM can use historical data analytics tools to gather data across the organization to understand how risks are being mitigated in real time. Low-code applications can help build a tailored risk identification process that includes risk inventory, risk assessment scorecards, and a risk measurement methodology.

*Gartner Forecast Analysis: Low-Code Development Technologies, Worldwide – October 2022.

Internal audit: Internal audit teams utilize low-code applications to easily create and track progress of action plans created for individual findings, nonconformities, regulations, and manual entries. They are not only planning and integrating the audit data in real time, but also recording the findings and communicating across the organization to draw accurate and full-population-based samples.

The low-code approach enables all three lines of defense to use the same platform and share data based on access levels as well as create their own separate apps.

Potential risks of low code

Low-code development is enabling businesses the agility to build applications faster, which are easier to maintain and don't entail interference from developers that need a lot of time to be onboarded. But new technology exposes businesses to new risks. As low-code development allows more users to develop applications, it creates new vulnerabilities that need to be taken into consideration:

Risk of untrained citizen developers

- Business teams and novice developers without the right level of training can introduce security vulnerabilities such as security misconfiguration, untrusted and unmonitored components, recurring production defects, and poor user experience and application performance. This would further burden the IT team to address these issues.
- Organizations should establish configuration baselines and validate that these are followed and monitor configuration deviations. Limit use to preapproved components, turn on in-built logging capabilities, and monitor to proactively detect errors and attacks. It is critical for organizations to define and set enterprise standards, frameworks, and governance for low-code application development platforms to protect the enterprise and its stakeholders. Training and enablement programs must be developed to cover standards applicable to regulatory, operational, and financial risks and compliance requirements. Setting up a low-code center of excellence (COE) is key to improving, adapting, and empowering citizen developers.

Lack of visibility and oversight of apps within the enterprise

- Due to the ease of access to the low-code platform and creation of applications, it is a challenge for organizations to keep an inventory of the applications created by citizen developers and to monitor them. It could also introduce "application sprawl"—proliferation of creating similar applications that duplicate functionality or purpose. Applications created by citizen developers no longer in their roles or with organizations may have no support to address issues arising from infrastructure changes, leaving organizations either exposed to threats or stuck with obsolete applications.

No or low auditability capabilities of low-code platforms

- Low-code platforms may be able to readily provide information necessary for audit purposes, legal discovery, and forensic investigations.
- To ensure low-code applications and platforms have relevant logging capabilities enabled and available for secure analysis, it is necessary to determine applicable compliance requirements to allow for detailed analysis to address audit and regulatory needs.

Lack of data management and platform governance

- Without appropriate access controls, low-code platforms can be accessible to anyone within an organization and the potential to expose sensitive, private, and confidential data is high, leading to regulatory fines and reputational damages.
- A robust governance framework ensures appropriate security controls throughout the lifecycle of application development. Companies must have procedures to securely manage application programming interfaces (APIs) interacting with developed applications. Defining and categorizing data is crucial to validate appropriate measures are in place to protect and encrypt sensitive data.

Third-party/vendor management risk

- With organizations increasingly adopting low-code platforms from various technology providers as well as utilizing third-party firms to build out applications, there is a gap with respect to clearly defined roles and responsibilities and procedures to monitor the activities of the third-party firms.
- It is critical to make sure that third-party vendors are trained on enterprise standards and guidelines and have access controls to enterprise data. Third-party vendors must provide attestation reports that can validate the controls they have in place to protect enterprise data and to update it on the backend when it comes to backups and restorations.

Building a "by design" mindset

We live in an increasingly interconnected world. Interconnectedness—technologically, financially, economically, socially, and environmentally—gives rise to interdependencies, making our risk landscape inherently more dynamic. The risk landscape comprises two key perspectives:

- The business perspective involves building applications for internal and even external users to optimize processes, respond to changing market needs, and interact with stakeholders.
- The risk perspective involves ensuring the quality of the application without hampering innovation or overburdening the RM function and still meeting the risk appetite.

Fast-changing business requires more agile and flexible RM. The RM function needs a business that is more risk-minded and knowledgeable on increasingly complex issues. To successfully deploy low-code applications within organizations and gain trust, leaders need to have a "by design" mindset. The most effective way for an organization to prepare for possible threats is to bring in risk mitigation factors as early as possible in the development process, as opposed to when they fully materialize. To level the playing field between risk and change, businesses need to:

- Have the requisite knowledge or access to the right sources to manage identified risks
- Establish agile RM to adapt and comply with evolving standards and risk procedures
- Replace manual workflows with technology enablement to reduce the burden on RM function
- Establish a governance process that reviews the application portfolio and an inventory management system to continuously track new and existing applications. Utilizing permissioned platforms using licenses or rules can help enable an oversight of all developers who have access to create applications.
- Build a generalized trust by design framework to accelerate innovation and digitization from a single source of trust.

Getting started while maintaining stakeholder trust

Since there are different inherent risks to different types of low-code application development within an organization, companies may opt for the following three key approaches to RM:

- **Solo zone** is a practical light-touch governance, and this is ideal for analysts who develop apps on their own, involving comparatively lower risks and low complexities.
- **Band zone** is ideal for developments where more people are involved and there is a need to review access periodically instead of allowing automated monitoring to take care of it. Within this zone, the project is deemed to be of medium complexity and low-medium risk. Citizen Development can solicit the support of the COE and its practitioners.
- **Orchestra zone** is suitable for applications with a high level of mission criticality, which is inherent to high risk or high technical complexity that requires continuous monitoring of internal and industry-standard controls.

Trust By Design framework

KPMG has developed a framework that allows businesses to have a risk-based approach instead of overloading the citizen developers and stifling innovation. Starting with ideation and opportunity creation to deployment, the whole risk lifecycle needs to be taken into account. This involves the assessment of risks, application of the right policies to these developments, risk mitigation with corporate guidance, and ultimately, reporting these risks to auditors while ensuring citizen developers are a part of this journey.

- For firms considering or in the process of launching citizen developer programs:
  - Obtaining an independent assurance on your low-code automation strategy
  - Assessing the program design, including policies, standards, and practices, and assessing the logic of development
  - Ensuring that all safeguards are mapped out during design and implementation, and following a controlled software development methodology
  - Performing a target operating model review in the context of examining your desired results for low-code-developed applications.
- For firms that are already operating a citizen developer program:
  - Identifying all existing applications and then assessing, categorizing, and prioritizing those that pose major risks to your firm
  - Determining the sources and outputs of data being used and then validating whether your data governance procedures are being applied in the gathering, handling, and generation of the data
  - Ensuring that security and privacy processes are implemented and operated effectively to minimize risks
  - Assessing and recommending improvement areas of training for developers.

KPMG Technology Risk Modernization – Centers of Excellence

As digital transformations accelerate in business functions at a record pace, our Technology Risk network has developed the KPMG Technology Risk Modernization COE to provide insights and help organizations evolve their capabilities to respond to risks associated with digital acceleration, cloud transformation, and emerging technologies. Our Technology Risk Modernization COE can help organizations with the following modernization efforts:

- Cloud technologies and governance
- Governance and observability for DevSecOps
- Low-code platforms, digital process automation, and quantum computing
- 5G and connected devices (IoT)
- APIs and microservices
- Cryptoassets and NFTs.

Learn more at visit.kpmg.us/TRMCOE.

Closing comments

Low-code platforms are becoming the unifying fabric of the digital enterprise—and the key to accelerating enterprise modernization, agility, and efficiency. As a result, citizen developers can now quickly develop sophisticated enterprise-class applications that incorporate complex business logic, automate workflow, integrate with existing information systems, and enable a slick user experience. While organizations deploy the latest technologies to drive growth, they must also recognize the risks that accompany them. To achieve successful transformation, establishing a data-driven culture, a robust RM and governance framework, and a COE is critical.

Contact us

Nana Amonoo-Neizer
Director
Technology Risk
T: +1 402-661-5316
E: namonooneizer@kpmg.com

Stefan Jacobs
Manager, Digital Excellence Hub
KPMG in the Netherlands
T: +31-402502329
E: jacobs.stefan@kpmg.nl

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.