KPMG

Citizen developer enablement

Managing enterprise risks while driving the adoption of low code

2021

kpmg.com

By 2024, low-code application development will be responsible for more than 65% of application development activity.[1]

The global low-code development platform market is predicted to generate a revenue of $187 billion by 2030, rising from $10 billion in 2019, and is expected to advance at a fast pace, 31% CAGR, during the forecast period.[2]

By 2024, 75% of large enterprises will be using at least four low-code development tools for both IT application development and citizen development initiatives.[3]

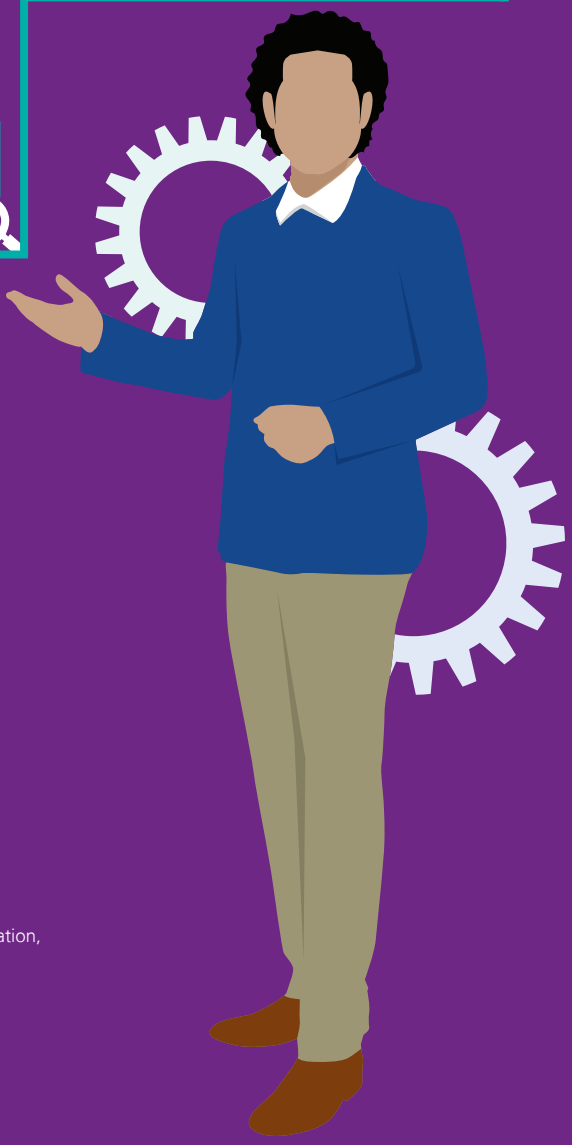
24% of low-code users had no experience at all before using low-code platforms. And 40% of users come from a mostly business background.[4]

42% of IT professionals plan to deliver 10 apps or more for their organization. However, the average time to develop these apps is five months or more.[5]

Nearly **60%** of all custom apps are now built outside the IT department. Of those, 30% are built by employees with either limited or no technical development skills.[6]

About **79%** of businesses build a web application with citizen development within a year.[7]

According to Forrester Research, by 2024 there will be a deficit of 500,000 software developers in the U.S. alone.[8]



KPMG insight

Low-code application development changes the conversation from years to months, weeks, and days. Without the right governance, risk, and control procedures in place, low-code will not live up to the promise of speed to market and could potentially expose organizations to unwanted risks.

[1] Gartner, Magic Quadrant for Enterprise Low-Code Application Platforms, August 2019

[2] Intrado GlobeNewswire, Global $187 Billion Low-Code Development Platform Market to 2030, November 2020

[3] Gartner, Magic Quadrant for Enterprise Low-Code Application Platforms, August 2019

[4] Mendix, Infographic: Low-Code Application Development Trends, July 2018

[5] Outsystems, The State of Application Development, 2018: How IT Is Responding to Digital Disruption and Innovation, July 2018

[6] 451 Research and FileMaker, Custom Apps – The Engine of Digital Transformation, August 2017

[7] Gartner, Magic Quadrant for Enterprise Low-Code Application Platforms, August 2019

[8] Forrester Research, Inc., How to Harness Citizen Developers to Expand Your AD&D Capacity, April 2017

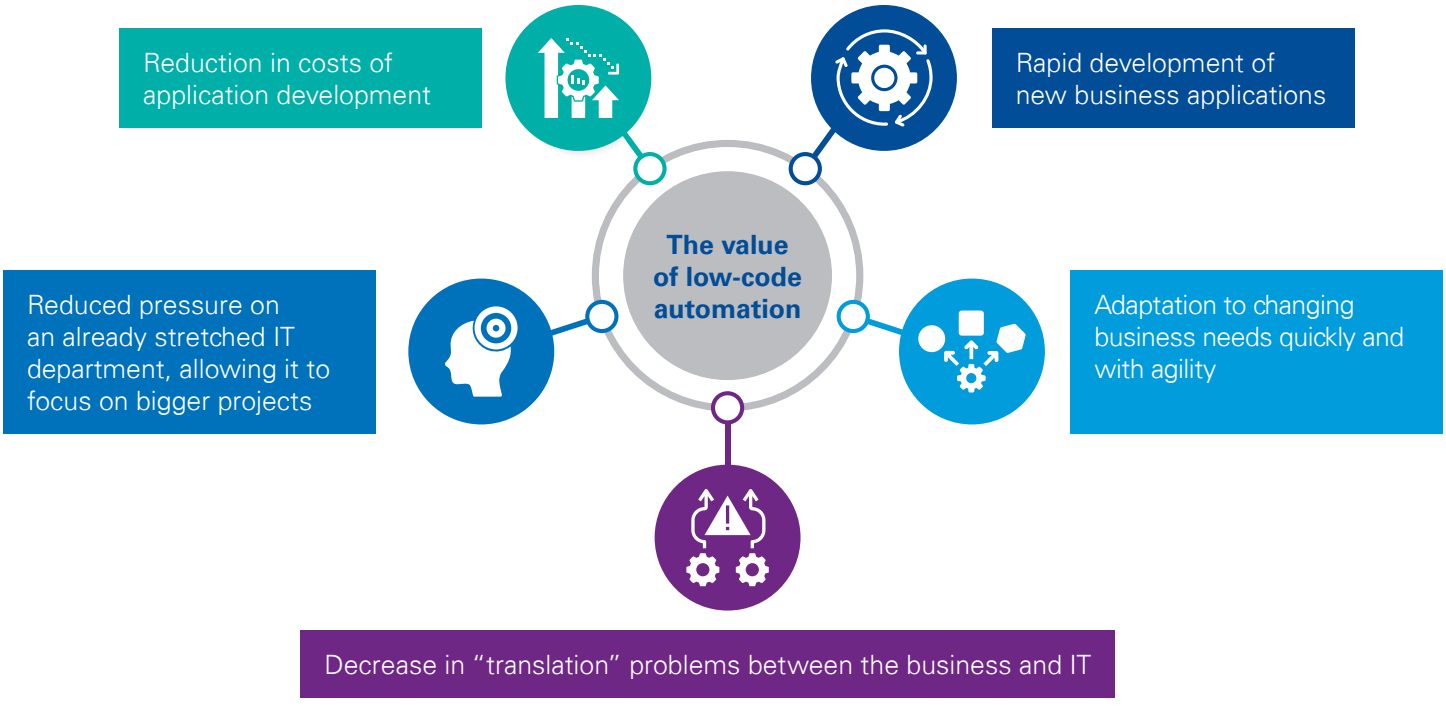
The citizen developer movement

Rapidly changing business conditions have driven the need to speed up digital transformation initiatives and business process optimization. Unfortunately, there is also an overwhelming backlog of application enhancement projects due to overworked and, generally, understaffed IT Development departments. According to Forrester Research, by 2024 there will be a deficit of 500,000 software developers in the U.S. alone.

As a result, a growing number of organizations are enabling "citizen developers," business domain professionals who understand the business process and challenges but may have little to no software development experience, to create business applications using low-code/no-code platforms to solve their business needs. Business teams are now building solutions that were previously highly dependent on IT resources, giving rise to this new class of citizen developers. Citizen developers will use IT-approved platforms and enable better collaboration between business and IT. *(It is important to note that citizen developer programs stand in stark contrast with what "shadow IT" groups do—use unapproved platforms to build customized applications.)*

The citizen development movement is empowered by the rise of low-code/no-code development platforms. Low-code/no-code platforms are visual software development environments that allow citizen developers to drag and drop application components, connect them together, and create mobile or web applications. *("Low code" will be used to represent both platforms in subsequent paragraphs and sections.)*

The surge in citizen developers and low-code automation is driven by the benefits they bring to organizations meeting the ever-changing needs and wants of customers and the market.



Low code in action

— A large retail bank in Australia transformed customer experience by rolling out 23 tier-one enterprise applications at a rate faster than one per month.[9]

— An international airport in the U.S. rolled out 18 new apps in nine months, averaging one new app every two weeks.[10]

— An innovative healthcare organization developed a spend management platform in under nine months with one developer.[11]

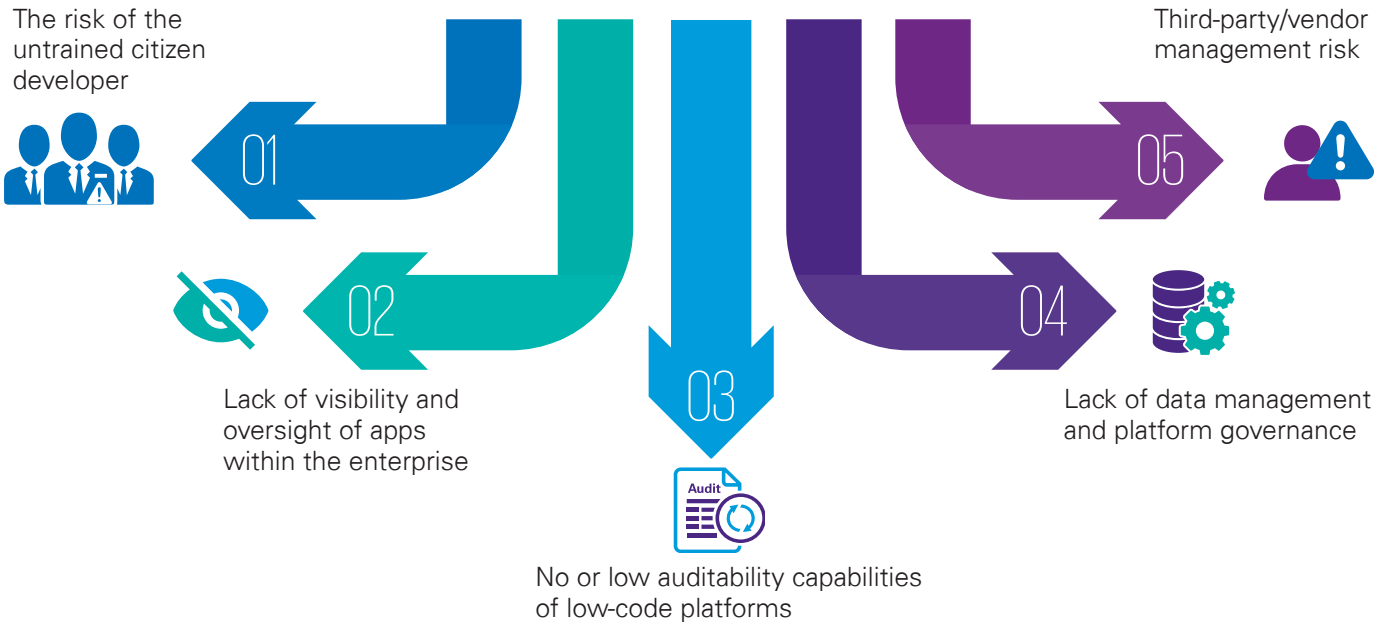
— A business development bank in Canada developed a loan processing app within eight months.[12]

— A financial services company created a loan eligibility app to facilitate relief under the Paycheck Protection Program (PPP) within six days.[13]

Governance, risk, and controls

The speed of application development—from ideation to the speed of application deployment—can provide a great boost to organizations. Conversely, organizations adopting and implementing low-code automation can expose themselves to potential risks.

The following are some of the potential risks and steps organizations can take to navigate these risks and turn them into opportunities.



[9] Appian, Examples and Use Cases of Low-Code, 2021

[10] Appian, Examples and Use Cases of Low-Code, 2021

[11] Mendix, Low-code. High Impact., 2021

[12] Mendix, Low-code. High Impact., 2021

[13] The Forrester Wave: Low-Code/Digital Process Automation Service Providers, Q3, 2020

1. The risk of the untrained citizen developer

Risk: Business teams and novice developers without the right level of training can introduce security vulnerabilities, recurring production defects, poor user experience and application performance, and inflexible or inextensible application. This would require the already overburdened IT security team to address these issues.

Considerations:

Define and set enterprise standards, frameworks, governance, and guardrails for low-code application development platforms to ensure consistent use and to protect the enterprise.

Start the citizen developer journey with a blended team of technology and business personnel to establish the low-code building blocks to be assembled toward the creation of business applications.

Develop ongoing training/enablement programs to cover standards that are applicable and relevant to regulatory, operational, and financial risks and compliance requirements.

Set up a low-code center of excellence to continually improve, adapt, and empower citizen developers.

2. Lack of visibility and oversight of apps within the enterprise

Risk: 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," i.e., proliferation of creating similar applications that duplicate functionality or purpose.

Considerations:

Establish a governance process that reviews the application portfolio and leverage reusable standards components.

Utilize role-based access control/permissions guidelines to determine all developers with access to create applications.

Establish an application library/management repository to continuously track new and existing applications.

3. No or low auditability capabilities of low-code platforms

Risk: Low-code platforms may not be set up to readily provide information necessary for audit purposes, legal discovery, and forensic investigations.

Considerations:

Define standards for low-code applications to allow for detailed analysis to address audit and regulatory needs.

Determine applicable compliance requirements and ensure that the low-code applications and platforms have relevant logging capabilities enabled and available for secured analysis.

4. Lack of data management and platform governance

Risk: 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.

Considerations:

Establish a governance framework that defines and sets appropriate security controls throughout the lifecycle of application creation.

Ensure procedures are in place to securely manage application programming interfaces (API) interacting with low-code developed applications.

Define classification standards for all types of data and metadata accessed by low-code applications. Define and categorize data to ensure appropriate measures are in place to manage and protect sensitive data.

Ensure platform companies provide attestation reports, security certifications, and other assurance to organizations over measures in place to protect data.

Ensure all data sources are defined and appropriate measures are in place to govern the collection, usage, and disposal of sensitive data.

5. Third-party/vendor management risk

Risk: As organizations adopt low-code platforms from various technology providers as well as utilize third-party firms to build out applications, many have not clearly defined roles and responsibilities and procedures to monitor activities of the third-party firms.

Considerations:

Ensure third-party vendors are trained on enterprise standards and guidelines and have access controls to enterprise data.

Ensure relevant vendor management procedures are applied.

KPMG final insights

Organizations will have to implement technology risk management procedures to the appropriate degree to ensure all stakeholders are protected while not hampering the innovative and fast-paced aspect of the citizen developer program. These procedures should allow citizen developers to take risks within the defined and acceptable risk boundaries to achieve the ultimate goal—improve time to market.

How KPMG can help you

Whether you are considering how a citizen developer program and low-code automation could benefit your organization, or you already have it in place and are looking for ways to refine and improve it, KPMG can help. Our highly trained professionals can support your technology risk functions by identifying actual or potential risks posed by applications developed through low-code automation and recommending appropriate controls.

For firms considering or in the process of launching citizen developer programs, we can:

- Provide an independent assurance on your low-code automation strategy
- Assess the program design, including policies, standards, and practices
- Help ensure that all safeguards are mapped out during design and implementation, and follow a controlled software development methodology
- Perform a target operating model review in the context of examining your desired results of the low-code developed applications.

If your firm is already operating a citizen developer program, we can help:

- Identify all existing applications, and then assess, categorize, and prioritize those that pose the greatest risks to your firm
- Identify the sources and outputs of data being used and then determine whether your data governance procedures are being applied in the gathering, handling, and generation of the data
- Ensure that security and privacy processes are implemented and operating effectively to minimize risks
- Assess and recommend improvement areas for training.

Learn more by visiting read.kpmg.us/TRM and read.kpmg.us/lowcode.

Contact us

Beth McKenney
Principal
Technology Risk Management
T: 313-230-3406
E: bmckenney@kpmg.com

Rey Villanueva
Principal
KPMG Digital Lighthouse
T: 312-543-6768
E: rqvillanueva@kpmg.com

Jason Glantz
Managing Director
Technology Risk Management
T: 973-467-9650
E: jglantz@kpmg.com

Raj Konduru
Managing Director
CIO Advisory
T: 216-224-3920
E: rkonduru@kpmg.com

Nana Amonoo-Neizer
Manager
Technology Risk Management
T: 402-661-5316
E: namonooneizer@kpmg.com

Maria Tachie-Menson
Manager
Technology Risk Management
T: 949-431-7212
E: mtachiemenson@kpmg.com

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