



# LOW-CODE GOVERNANCE

Foster Innovation, Speed Up  
Development, Maintain Control





# TABLE OF CONTENTS

## Your Recipe for Success

If you're here, chances are you're considering a low-code platform or already using one. To get the most value out of that investment, you need a new way of thinking about governance. That's what this book is for. Read on to discover why low-code governance matters and how Mendix provides you world-class ingredients throughout the development lifecycle, leading to a secure, flexible, adaptive, and frictionless user experience.

- 03 | INTRODUCTION
- 04 | WHAT IS LOW-CODE GOVERNANCE?
- 05 | FROM "GOOD ENOUGH" TO "EXCEPTIONAL"
- 06 | HOW TO STRUCTURE YOUR CENTER OF EXCELLENCE
- 08 | COE ROLES: EXCELLENT PEOPLE POWER EXCELLENCE
- 10 | THE TRACK TO GOVERNANCE
- 17 | GOOD GOVERNANCE DONE RIGHT

## Introduction

Building a healthy and thriving low-code enterprise software portfolio is a lot like cooking a meal. You can have the best ingredients, but if you don't have the right recipe to put them together, you create risks, like risk of a security breach or making something that doesn't create value.

But with the right tools to form your governance strategy, you have your manual and your experts, setting yourself up for a great meal. Governance, in essence, provides the guardrails and visibility to minimize risk while creating value. It's about attaining and maintaining **focus, command, and control**. Governance is as critical to your landscape as your architecture, data, and anything else.

When you can get your governance plan and execution to the right spot, you foster innovation, enable scale, enhance developer productivity, and boost business confidence.

Mendix has been a leader in the low-code space for nearly 20 years, and we understand the importance of governance to your applications and your entire portfolio. Governance is your framework for success, and in this book, we'll show you **why low-code governance is so important, how to structure it for your organization, and how you can map your journey**. You'll also meet a fictional company as they navigate their own low-code governance path.

So get your utensils and appliances ready, and let's see how to use governance to accelerate your low-code impact.

### Growing Governance @ Cacti

Cacti Insurance is a young insurance firm. The company's CEO has laid out an ambitious growth plan. Realizing that plan means transitioning to a digital-first organization. Such a plan requires the whole organization to build customer-facing apps for things like signing up for insurance, checking status, and making claims.

For the CIO, this strategy means rethinking how Cacti manages its development and digitizes its business. Governance is especially critical to Cacti because of a complex and evolving regulatory environment.

Currently, Cacti uses Mendix's low-code platform for three apps in their organization. Mendix was a

great choice because of its [commitment](#) to security, governance, data privacy, and compliance. However, most of Cacti's development is still rooted in traditional practices.

Cacti has identified another dozen opportunities in their organization where Mendix could help them modernize and move away from legacy applications. They're hiring eight new Mendix developers to help. But, before starting new development, they need a governance plan that covers their whole app landscape, ensures security, compliance, and quality, and helps reduce costs and optimize value.

We'll check back in on Cacti in a bit!

## What is low-code governance?

Low-code helps enterprises develop better software at speed and scale. That's just one of the reasons why more and more organizations are using it. But a single use case, or even a few apps, is just the start. Do you want to enable your teams to do more with your low-code platforms? **Governance is vital to enabling success at scale.** It will help you deliver business value at acceptable risk and cost. It's like finding the right combination of spices to make your ingredients the best they can be.

**Governance:** The tools, policies, and procedures that help minimize risk and ensure quality, consistency, and security in low-code development.

**Governance is about having oversight and maintaining control over both a landscape of apps and individual app development.** Increase accountability, increase transparency, and get the most ROI out of what your teams build and deploy. **Lack of governance is what leads to shadow IT.**

Governance helps you achieve your goals without compromising security or quality. It will help you answer questions such as:



**Guidelines and oversight:** Is your organization clear about common, best dev practices? Who's responsible for software quality? How can you monitor these areas?



**Security risk:** How do you view and remediate security vulnerabilities impacting your application landscape?



**Investment control:** How can you ensure that technology is aligned with business goals and delivering a positive ROI?



**Time + effort:** Are you using reusable components to make the most of your developers' time?



**Value:** Can you prove how your app contributes to business goals with tangible, data-driven insights?

Put another way, low-code governance is the bundle of tools, policies, and procedures your organization applies across your entire app landscape and development lifecycle. **Effective low-code governance helps ensure your people and applications are secure and compliant and enables effective scaling and rapid outcomes.**



### FOOD FOR THOUGHT

*WHAT DOES GOVERNANCE MEAN IN YOUR ORG? WHO'S INVOLVED? WOULD YOU CONSIDER YOUR CURRENT GOVERNANCE PRACTICE EFFECTIVE? WHAT'S YOUR CORE MISSION?*

# From “good enough” to “exceptional”

Getting organizational governance right requires someone to be responsible for its execution.

A **Center of Excellence (CoE)** can help lead and set the way for your governance strategy.

**CoEs** generally ensure that stakeholders from throughout the business and IT **collaborate, commit to, and execute plans, priorities, and guidelines** that will drive business goals while maintaining standards and best practices for development.



**Center of Excellence:** A team in your organization responsible for a specific platform or focused on a particular business domain.

Another common way to think about collaboration is with fusion teams. **Fusion teams** tend to focus more on the app cycle, while CoEs concentrate on the portfolio cycle. We'll cover more on that later.



**Fusion Teams:** Collaborative cross-functional teams made up of people with various digital talents, disciplines, and skill sets.

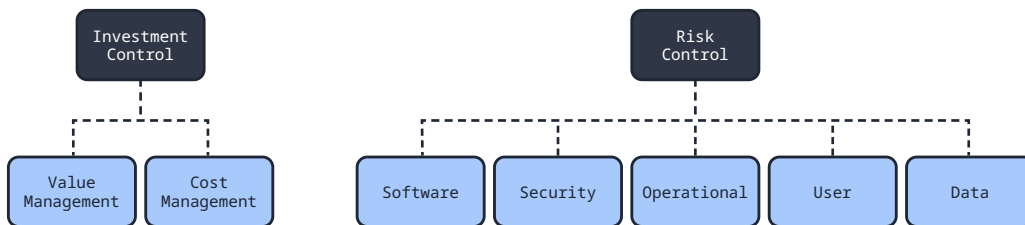
Let's be very clear about one thing before we proceed: your governance objectives, stakeholders, and structure will all be unique to your organization. Everything we're talking about here is one approach illustrating the use of built-in platform capabilities. If your org matches the below exactly? Great! If you're seeing just shades of your business in there? That's fine. In-built governance capabilities are flexible and can be tailored to your needs.

**The point is understanding why CoEs matter and how to set yourself up for success.**

And don't worry! It doesn't have to be a huge operation.

The governance objectives of a typical CoE are pretty straightforward:

- **Investment Control:** Maximize return on investment on your platform tooling. Proactively control costs and measure business value.
- **Risk Control:** Build sustainable software with acceptable risk. Set common guidelines and standards for software dev, security, operational health, user management, and data.



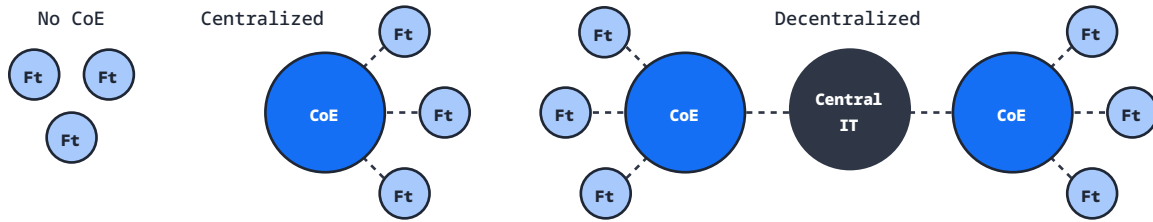
Investment controls help to manage costs and business value. Risk controls help mitigate risks across the entire development lifecycle.

## Growing Governance @ Cacti

With just a few apps live initially, Cacti didn't have a CoE. At the time, this was okay because the teams were small, and business/developer collaboration was simpler. However, with new Mendix developers getting onboarded and the many new apps that need to be built with new departments, they need a central body to own the Mendix platform and set guidelines and guardrails to help scale effectively.

# How to structure your center of excellence

There's no right or wrong answer to structuring your CoE, but a few options exist. Depending on the size of the organization and resources, here are a few ways to position it:



Ft = Fusion Teams | CoE = Center of Excellence



## No CoE

If you work for an organization with a smaller IT footprint, a CoE may not be necessary. If your software portfolio is just an app or two, there's no need to overcomplicate it. That said, if you want to scale your operations, you'll want to get a CoE started sooner rather than later.



## Centralized

Here, responsibility and all development initiatives sit with central IT or a CoE. The benefits are clear: **visibility, control, and efficiency**. Business units and other requestors can request central IT, but IT ensures your standards and processes are in place. **We recommend starting to think about your CoE in a centralized way** because of the simplicity of the setup. Drawbacks to a centralized CoE come if your enterprise is large, multinational, or has a lot of distinct business units that operate independently. You quickly run into bottlenecks: too many questions and not enough people to deal with them efficiently.



## Decentralized

In a decentralized CoE, central IT is responsible for the more technical aspects of governance, such as architectural decisions or security requirements. From there, individual business units (BU), which likely have their own IT orgs, stacks, and funding, take over. So, the individual BUs could be responsible for things like integrations, security implementation, investment control, risk control, requirements, feedback, and more, while the overall guidelines come from the center. There's no one-size-fits-all here, as the mix will vary depending on the business.

**The key is that central IT is responsible for ensuring compliance across the various BUs, while the BUs are responsible for ensuring their projects maintain the compliance set by central IT.**

Depending on the organization's needs, you can transition from centralized to decentralized and back and forth. It probably will save you a few headaches to not change around constantly, but you need to be tuned in to the needs of your enterprise.

Ultimately, your CoE is in place to ensure fast, secure development. After all, isn't that your end goal? Focus less on the structure and more on getting the right people in place. Who are the right people? Read on to find out.



### FOOD FOR THOUGHT

*THINK ABOUT YOUR ORGANIZATION. WHAT KIND OF COE DO YOU THINK FITS YOUR ORG BEST? WHAT BENEFITS COULD YOU SEE? ANY POTENTIAL CHALLENGES?*

## CoE roles: Excellent people power excellence

Think of a professional kitchen, the kind you might see in any restaurant. Most aren't run by a single person. A more standard structure is someone calling out orders, separate people working on different stations like the grill and the fryer, and someone to take care of the final plating and quality control. **When everyone works in their role, the team can get more done** and create a better product. If not, they're getting in each other's way and risking sending out lousy food. Your CoE roles work precisely the same way.



### Central IT & CoE

#### Responsibilities

- Ultimately responsible for the success of technology investments and ensuring fusion teams can focus on their initiatives.
- Define dev guardrails to mitigate vulnerabilities and limit risk, including security best practices, deployment processes and policies around integrations, quality assurance, etc.
- Turn best practices into reusable components or templates to ensure quality and consistency across the app landscape.
- Prioritize projects, making sure they tie to business priorities and that any app delivers on its purposes.

#### People who can/have

- Translate organizational strategy into development standards, policies, and guidelines.
- Collaborate closely with business stakeholders to identify and prioritize opportunities aligned with business impact.
- An architect, business, or IT-type background.
- Expertise in data protection and security regulations relevant to the organization.



### Fusion Teams

#### Responsibilities


- Actual development and delivery of apps, including maintenance.
- Making sure apps fulfill functional requirements via collaboration with different stakeholders.

#### People who can/have

- Technical know-how, can develop according to guardrails defined by Central IT and CoE.
- Subject matter expertise (SME) for areas where apps are being developed.
- Capability of empowering teams to focus on getting dev done.

**Getting your CoE started is as simple as pulling the right people together.** Designate a CoE Lead who can own the process and bring in relevant developers and business stakeholders to help prioritize business needs.

Let's put this into action. Suppose you're working in a centralized CoE. In that case, your business stakeholders work with the CoE Lead to identify high-impact opportunities, the CoE sets guidelines, and fusion teams of developers and **business technologists** build out applications.

 **Business Technologist:** A non-IT employee creating applications for either internal or external (customer-facing) use.

In a decentralized CoE, the CoE still provides overarching guidance to empower users to deliver their own projects. Still, fusion teams are much more empowered to design and maintain their own practices.

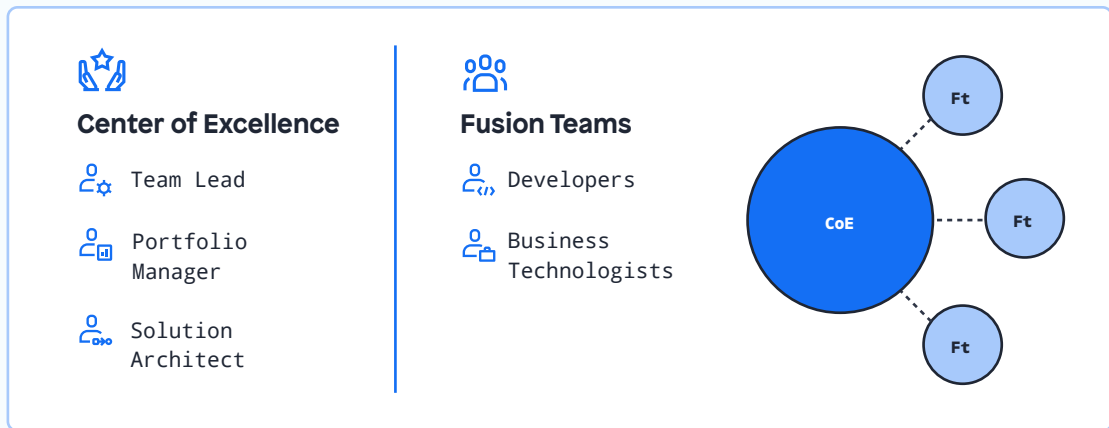
### Growing Governance @ Cacti

Governance at Cacti has historically run through a single team lead. They're fantastic and know both the business and regulatory needs inside and out while having generous experience in the software development domain, including Mendix.

However, with the shift from legacy apps to modern low-code apps, there is a lot to be done. With

multiple new fusion teams forming, Cacti has created a centralized CoE to define guidelines, guardrails, and best practices and to help evangelize the platform aimed at getting the most out of the platform.

In addition to the team lead, a portfolio manager and a solution architect have joined forces to form the initial CoE. This CoE is responsible for all Mendix low-code application development.





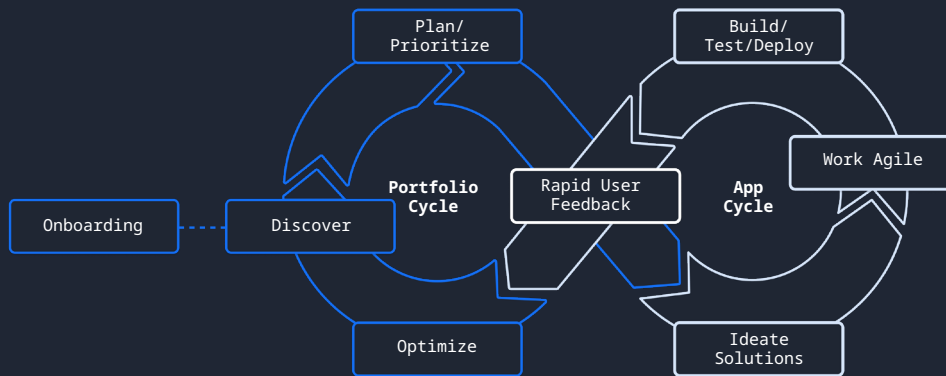
# The track to governance

Having your people in place is an enormous piece of the puzzle. But they must be supported by platforms and processes that make governance simple.

At Mendix, we look at governance as a never-ending journey. Continuously monitoring and adapting to changing needs is the norm. Even better? Governance is baked into the platform, ready to go! If needed, you can also tailor capabilities to your needs.

Your **portfolio cycle** involves identifying, developing, measuring, and optimizing your applications. Your **app cycle** involves turning your priorities into value-driving solutions and then bringing learnings back to the portfolio.

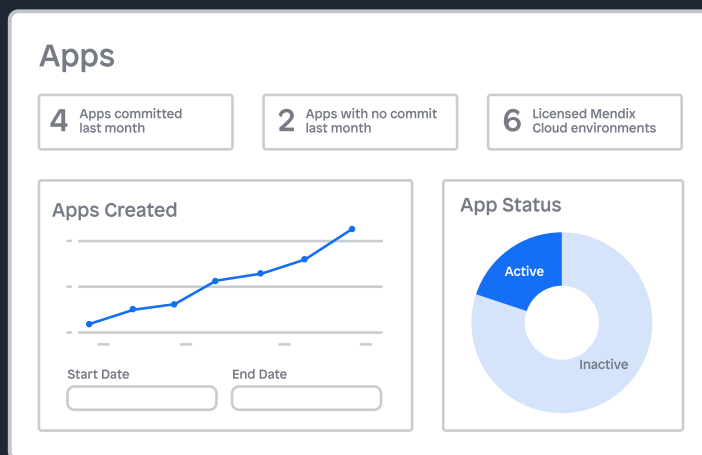
Not bad, right? Let's look at each step of the journey, why it matters, the Mendix capabilities to help you accomplish your goals, and how our friends at Cacti are working through them.



## Onboarding

Knowing the broad strokes of the Mendix platform early on is instrumental in getting early success. Onboarding is the first step of getting started with Mendix, where you implement the basics of using the platform and set the foundation for platform access and company branding.

[Control Center](#) is the primary tool for managing your Mendix app landscape. Control Center includes visibility into the apps you create, Mendix version, and member information, including users in the platform and their activity, along with controls to define settings & guardrails. When setting up governance, exploring and familiarizing yourself with Control Center is critical.



Control Center shows your landscape's status, members, and other key details.

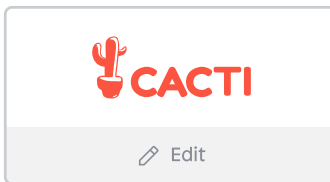
## Growing Governance @ Cacti

Cacti's three-member CoE have all just become admins in Control Center. They're now ready to focus on Cacti's portfolio cycle. They can also view and manage the employees within Cacti who are exploring or building apps on Mendix, helping them identify potential Mendix power users. However, they also find a Loan Assessment app created by an Account Executive that looks like shadow IT. Insights like these will help the CoE govern development even when it's happening outside central IT.

The CoE quickly tailors Mendix to their specific governance needs by:

### Company Brand

#### Logo



[Defining a company brand](#) by uploading Cacti's company logo and cover image. This quickly reflects across the Mendix platform, including on the [Developer Portal](#) and published marketplace content. All Cacti makers get a familiar look and feel now.

[Assigning a security contact](#) who is informed if there are critical security issues with the platform and platform-supported Marketplace components.

[Registering additional email domains](#) because Cacti's US office uses cacti.com while the Netherlands office uses cacti.nl. Registering the email domains in Control Center ensures that users signing up with any of these email addresses are recognized as Cacti employees, and the CoE can oversee their apps and activities in one place.

[Enabling Single Sign On \(SSO\)](#) for a frictionless login experience. More importantly, it's also more secure, given the login experience is connected to Cacti's identity provider. When a Cacti employee leaves, they are deactivated at the identity provider and lose the ability to log in to Mendix. And all this can be done by following a simple, guided wizard!

There's still lots to do, but the CoE is off to a great start. They give themselves a well-earned pat on the back.

### Company Settings

#### Security Contact



No security contact has been added yet.

Add security contact

### Single Sign-On

#### Active Configuration

Add Configuration

Azure AD

- Configuration tested
- Mapping configured

### Company Email Domains

Add Domain

cacti.com

cacti.nl

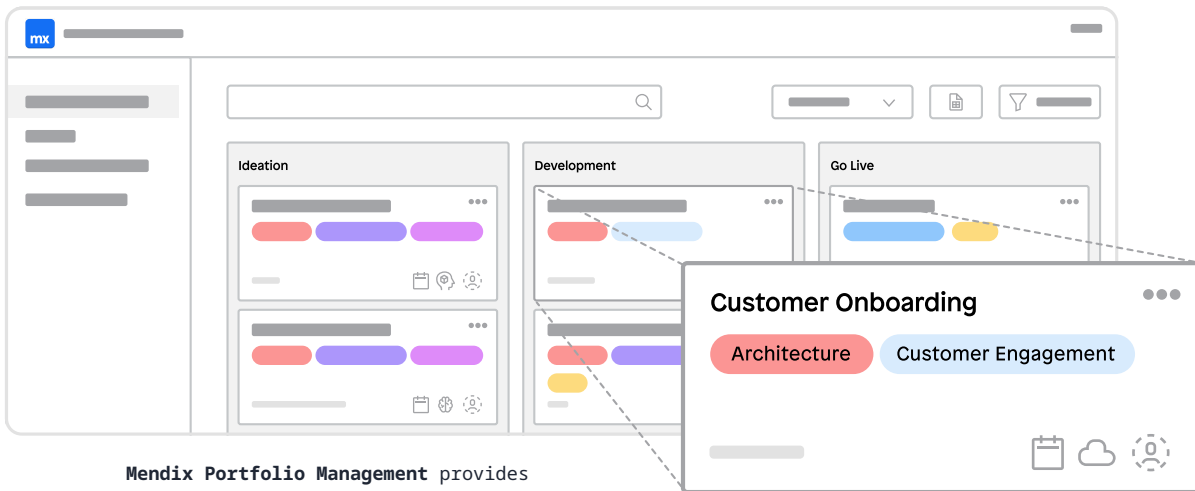
## Discover

Examine what business initiatives fit your low-code platform. Ideally, you're looking for opportunities that you can get to market quickly and will have a tangible impact on your business.

Cacti learned from the [Digital Execution Practice](#) that they should prioritize apps that will make an impact, can go live quickly, and always lead back to their broader business strategy. After a few brainstorming workshops, Cacti has consolidated a list of 15 definitive app requests, ranging from data management to a loan origination orchestration app. They have a good vision for how these apps will contribute to their digital transformation efforts but now need to figure out which ones to start with first.

## Plan & Prioritize

**Consciously plan & prioritize your initiatives consciously to maximize impact.** To unlock the full potential of the Mendix platform and accelerate your journey into digital transformation with low-code, Mendix provides various assets, including a [Digital Execution Manual](#) and platform-native Portfolio Management.



**Mendix Portfolio Management** provides insights to help teams plan and prioritize.

Cacti's CoE has organized all ideas using [Portfolio Management](#). While brainstorming during the previous Discover step, they started creating initiatives and assigning initial owners to their ideas. With built-in industry-leading prioritization methods like RICE, the CoE decides to begin with an Underwriter Workbench. This portal integrates disparate data sources and provides access through a single connected platform.

Next, they would need to staff the project with the right talent. In the [Members pane](#) in Control Center, they can view the certification levels of each maker at Cacti, including any externally hired consultants. Since viewing certification levels of internal and external members is possible in-platform, it helps get the right talent together.

## Ideate Solutions

Here, you're breaking the goal into smaller milestones. Who are the target users? What are current pains and future wishes? Getting on the **same page early and often** strengthens the group's focus and connections.

The app team is workshoping with their end users and stakeholders this week. The CoE provides them with a few tools:

The [public marketplace](#) has reusable modules, widgets, templates, and other content built by Mendix, partners, or community members. Sure enough, the team finds the [Underwriter Workbench](#). This template, built by Mendix and Capgemini, helps underwriters perform a risk assessment, including a predictive analysis.

Overall, the Underwriter Workbench could be a great starting point that can be tailored further to Cacti's use cases!

Cacti's [private marketplace](#) includes Cacti-specific reusable (and CoE-approved) content. Another team already built a risk assessor tailored to Cacti's business and published it as a module for reuse. That could be a valuable piece for the underwriting app.

[Mendix Academy](#) helps users up their skills and learn about new features. Different learning paths help in various use cases, such as [going mobile](#).

The screenshot displays the 'Company Content' section of the Cacti Private Marketplace. It features a search bar at the top and a grid of reusable modules. A callout box highlights the 'Cacti Risk Assessor' module, which is described as a 'Risk assessment module for the underwriting program' and is marked as 'Private'. Other visible modules include 'Approval Module', 'Image Uploader', and 'NL address from postcode'. Each module card includes a title, a three-dot menu icon, and a lock icon.

**Company Content**

**Cacti Risk Assessor**  
Published: 26 Jan 2024  
Risk assessment module for the underwriting program  
Private

Cacti's **Private Marketplace**, where they can internally share apps and app components for easy reuse.

## Work Agile

Agile is tried and tested in development, and that's because it's effective. According to Gartner, 96% of fusion teams use Agile methodologies. **Having the proper guidelines and guardrails helps the team focus on initiatives and outcomes.**

A new Mendix developer has joined Cacti. The Cacti admins can quickly onboard the new member by assigning them a [default role](#) and the apps they would need access to. Alternatively, the scrum master can add the new developer to the team with the required roles and permissions. It's quick and easy.

Cacti admins are also concerned about shadow IT and have seen at least one instance of it. Being a highly regulated firm, Cacti would like to ensure that only employees under its Digital Transformation Office (DTO) get access to create apps in Mendix. What's best? This can be set up in Cacti's [identity provider](#) and automatically applied to Mendix.

## Build, Test & Deploy

This is the big one. Here, you're building, testing, and getting your solutions out the door. No matter your CoE structure, **development teams must be empowered to develop and deliver effectively.** Standard integrations, reusable components, and an intuitive software release process become critical here.

The team at Cacti is all-hands on building their app, including the Underwriter Workbench they got from the marketplace. The CoE has also recommended using the [MxAssist Best Practice Bot](#).

### MxAssist Best Practice Bot:

Inspects an app in Studio Pro against Mendix best practices, detecting and pin-pointing dev anti-patterns and in some cases, automatically fixing them.

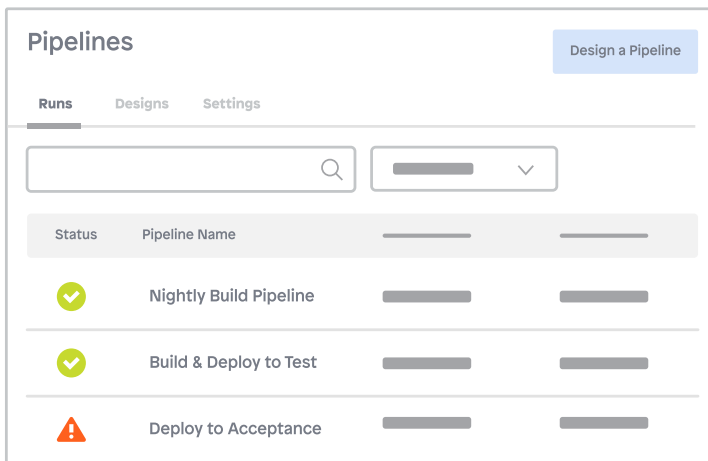
The team uses [Mendix Quality and Security Management \(QSM\)](#) to further ensure quality and secure software creation.

The team is further asked to provide the ability to audit data changes, access activity, and platform activity. Platform activity can be audited easily by exporting the [Activity pane](#) from various pages covering role and permission changes and deployment activity. Access activity can be audited via [application and access logs](#). The CoE suggests the [Advanced Audit Trail](#) module for data availability, which helps configure and track data-related changes along with infinitely scalable and fully-indexed data search.

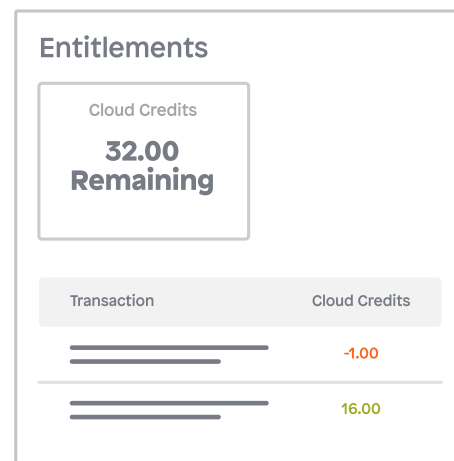
Fast forward a few days, and the team has a minimal viable product (MVP) ready to be tested. With one click, they push the app to the Acceptance environment and perform end-to-end, integration, and user acceptance testing. The app is then pushed to the Production environment and into the hands of the underwriting team, the key end users of the app. The CoE has advised the team to use [Pipelines](#) to fully automate packaging & deployment in the future so

that they can save precious development time, reduce manual effort & get more reliable deployments.

When the team needs a new environment, they can request one from the admin team. Using Control Center's [Entitlements](#) tab, the Cacti admin team provisions a new environment of their chosen size. This self-service tool helps make the most of their Mendix Cloud instance by providing the team with flexibility to optimize their cloud deployments.



With **Pipelines**, you can design your own build and deployment processes with easy-to-use, configurable, pre-built steps.



**Entitlements** provide flexibility to optimize Mendix Cloud deployments.

### Rapid User Feedback

To make an impactful solution, you need feedback. Ideally, you need it from all levels of stakeholders, and you need it aggregated and quickly.

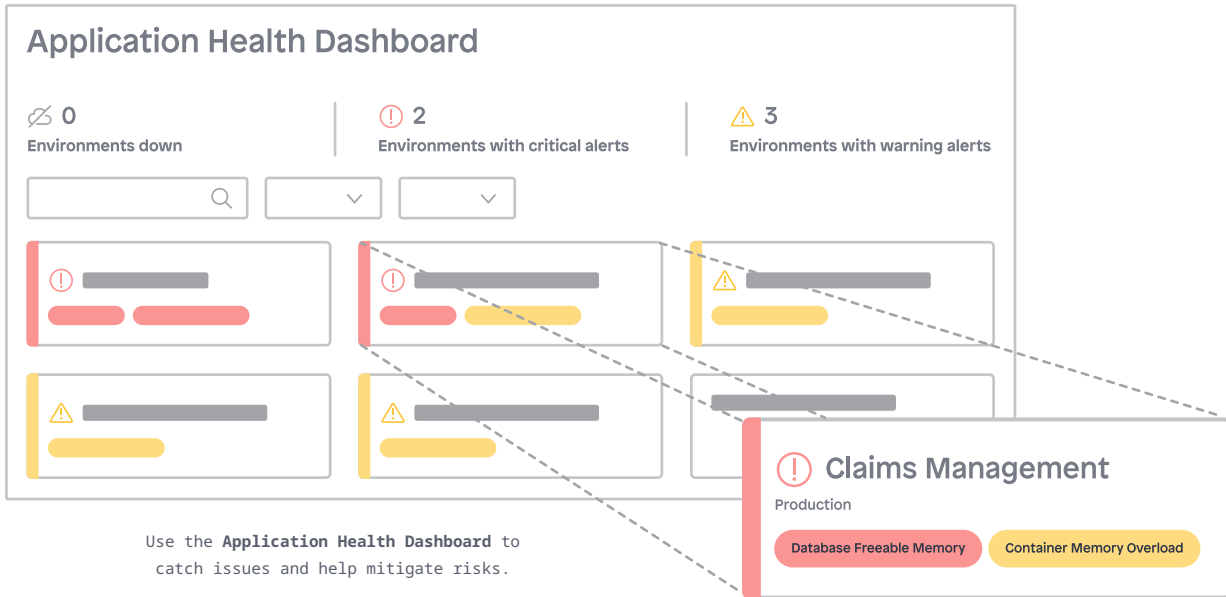
**A manageable way to get and track feedback is mission-critical.**

Cacti believes in being extremely user-centric. It's a proven philosophy that has helped them succeed in the market and differentiate from the competition.

Now that the app is launched, the team decides to use the CoE-recommended [Feedback module](#). This allows end-users to provide descriptive feedback, including images and annotations in-app. The app teams can evaluate these and convert them into stories to be implemented in upcoming sprints. A [Mini Surveys module](#) further helps collect feedback through in-app surveys.

## Optimize

It's important to **consciously manage a growing portfolio of apps, maximizing value, optimizing cost, and mitigating risks proactively**, learning from experiences and propagating that across your organization.



Fast forward a few months. Cacti now has six apps live, with three more in development. Cacti admins are more focused on optimizing across their app landscape now. Here's what they've been up to:

- To mitigate security risk, they have subscribed to notifications about security vulnerabilities. When a security vulnerability is detected, they identify the impact radius using [Software Composition](#) analysis and ensure remediations are done quickly. The Cacti CoE can view all the unique marketplace modules, widgets, and Java libraries used in their landscape, along with analysis. This helps Cacti admins find other highly used content that helps them refine their procedures.
- To mitigate software risk, Cacti created a **Starter App** template. As the name suggests, Cacti's developers can start with this app to benefit from basic Cacti-specific capabilities, design, and must-have marketplace content. Additionally, Cacti CoE regularly views the static code analysis dashboards from **Mendix QSM**.
- To ensure user maturity, they regularly review the state of their **certification levels** in Control Center and set goals for the future.
- To mitigate operational risk, they use the [Application Health Dashboard](#), which lays out alerts and warnings. This helps them follow up with relevant teams.

## Good governance done right

When everything's running well, governance can be the best cookbook you've ever had and the process can be adaptive, collaborative, and a value add. But forget to put the ingredients together at the right time, or even miss an ingredient, and it becomes a huge headache very quickly.

Governance done right enables your enterprise to deliver better software faster. Mendix, with our platform and our processes, helps you get there.

**Governance doesn't have to be complicated. Make the most of it with Mendix.**

### About Mendix

Mendix is a leader in low-code enterprise application development and recognized as a Leader in Gartner's Magic Quadrant for Enterprise Low-Code Applications.

Mendix is the only low-code platform capable of handling the most demanding and complex organizational challenges.

Read more about the Mendix platform and how it can drive your organization forward. [Speak with a Mendix representative](#) to learn how your business can start today.

