

Ignition Guide to Initiating a Cloud-Native Journey

Peer & Practitioner Research Published 21 October 2022 - ID G00778541 - 19 min read

Enterprise Architecture Research Team

Initiatives: [Technology Innovation](#); [Enterprise Architecture](#)

Modernizing systems to be cloud-native requires fundamental improvements to processes, culture and measurement. This Ignition Guide provides enterprise architecture and technology innovation leaders with the tools necessary to develop and implement a business-driven cloud-native strategy.

Additional Perspectives

- [Summary Translation: Ignition Guide to Initiating a Cloud-Native Journey](#)
(23 November 2022)

Overview

This guide will help you:

- Build a comprehensive cloud-native strategy based on targeted business outcomes.
- Operationalize the cloud-native strategy with an implementation roadmap and facilitate accompanying change management.
- Achieve agility and cost efficiency through optimized cloud operations.

*This Ignition Guide is tailor-made for short-cycle projects that take between a few weeks to a month to execute and may not require extensive planning to get started or monitoring after launch.

ESSENTIAL Steps marked as Essential have been identified as critical for the successful execution of this project.

Steps

- | |
|--|
| 1. Align cloud-native strategy to business objectives. |
| 2. Develop the strategy. |
| 3. Implement the strategy. |
| 4. Measure performance and make improvements. |

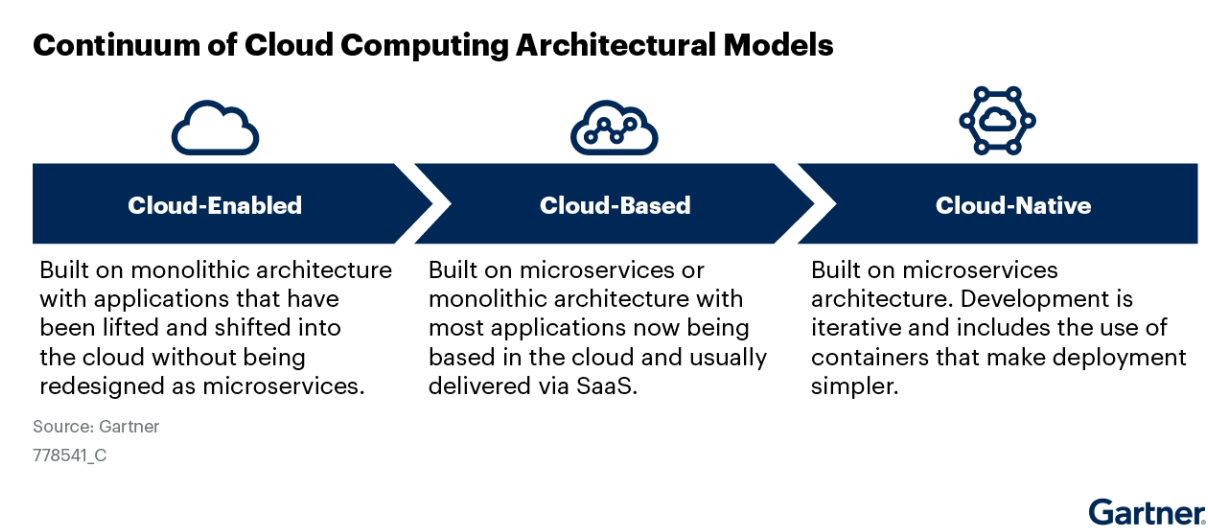
Before You Start

A list of terms used in this research, along with their definitions, can be found in the [Download Attachments](#) section.

Make sure you have the following resources:

- Ability to develop solutions iteratively using a minimum-viable-product (MVP) approach and embedding security in all aspects of design.
- Access to technologies that enable observability of how applications are being used and behave in the cloud.
- Ability to leverage open-source solutions to more effectively integrate cloud-native applications across public, private and hybrid environments.
- Establish a governance model with a defined set of policies that ensure appropriate permissions for individuals who need access to the cloud development environment.
- Understanding of or familiarity with cloud computing models (see Figure 1).

Figure 1. Continuum of Cloud Computing Architectural Models









Use Figure 2 to assess your readiness to go cloud-native. The assessment below is not an exhaustive list of needs; it is meant to serve as a starting point for developing your criteria to consider. This Ignition Guide will more thoroughly examine each of these components in further detail in later sections.

Figure 2. Assess Your Readiness to Go Cloud-Native

Assess Your Readiness to Go Cloud-Native

Use technical, operational and organizational change criteria to assess whether you can initiate a cloud-native journey.

| | | | |
|---|---|--------------------------|--|
|  | Do I have a plan to allocate resources and manage costs (migration costs and management costs)? | <input type="checkbox"/> | Use the Ignition Guide to identify potential stakeholders from whom you will need buy-in and support. |
|  | Do I have stakeholder buy-in and support? | <input type="checkbox"/> | |
|  | Do I have a talent pipeline to implement the cloud-native strategy (short- and long-term)? | <input type="checkbox"/> | Cloud-native optimizes existing cloud-based computing; you will need to assess your existing cloud infrastructure. |
|  | Do I have the infrastructure to shift cloud-native (security, provider, deployment model, storage, etc.)? | <input type="checkbox"/> | |
|  | Do I know what stakeholder priorities and business objectives are? | <input type="checkbox"/> | |
|  | Do I have a cloud-native strategy and implementation roadmap to provide to my team and to stakeholders? | <input type="checkbox"/> | |

Source: Gartner
778541_C

Gartner

Common Pitfalls and Keys to Success

| Common Pitfalls | Keys to Success |
|--|--|
| All-or-Nothing Approach Enterprise leaders struggle to determine which applications and assets need to be run in the cloud and which do not, defaulting to the philosophy that they either all need to be cloud-based or not. | Focus on Generating Incremental Value Early Invest as you scale rather than deliver a large investment upfront. Starting with a narrow, well-defined use case first helps evaluate whether it will generate the intended business outcome, gauge talent and technical issues and plan for future scalability. |
| Insufficient Understanding of Intended Value and Anticipated Costs Lots of hype and technicalities exist around cloud-native, which makes it difficult to understand what cloud-native is, how much it will cost and how it can be used to provide return on investment. | Implement Monitoring and Diagnostics From the Start Prior to adoption, establish mechanisms to monitor and assess usage of cloud resources and total expense to align cloud-native strategy to business objectives and to ensure sufficient understanding of intended value. |
| Failing to Consider Organizational Nuances There is no single tool, delivery model or vendor that is appropriate for all organizational contexts; while some tools, delivery models and/or vendors might have worked for other organizations, mimicking those may not solve your enterprise's business objectives. | Actively Meet Organization-Specific Demands Placed on Cloud-Native Systems Continually conduct capabilities and requirements analysis to discern the right approach to achieving your intended outcomes. |
| Not Planning for Cultural Change Considering cloud-native as an "IT only" initiative focuses solely on the technical perspective, which could lead to resistance from business partners that can delay progress. | Engage All Relevant Stakeholders to Communicate Objectives and Potential Disruptions Stakeholders must have clear visibility of changes to ways of working and must have a chance to articulate needs or requirements directly. |
| Overdependence on a Platform or Provider's Security Services Cloud service providers may not always provide the right array of capabilities and services that the enterprise needs, particularly when it comes to security. Committing to a single provider prematurely could lock the enterprise into capabilities and services ill-suited to business objectives or compliance restrictions. | Implement Security Across the Entire Life Cycle of an Application From design and implementation to deployment and operations, focus on identity management, infrastructure access, application security and data sovereignty and encryption. Assess potential providers and capabilities and look for multivendor strategies, as long as these meet business and technology expectations. |

Step 1 of 4: Align Cloud-Native Strategy to Business Objectives

A cloud-native strategy involves rearchitecting legacy applications to be cloud-native or rebuilding/building a cloud-native version covering the monolithic application functions. Tailor your cloud-native strategy to your organization's readiness to implement it.

Tasks

1.1: Identify key stakeholders.

Develop a good understanding of the most important stakeholders to consult, how they are likely to respond to changes and how to win their support. Table 2 is an illustrative list of potential stakeholders to consult and of their likely contributions, but there may be other teams involved or overlapping responsibilities between teams that are organizationally dependent.

Table 1: List of Potential Stakeholders to Consult

(Enlarged table in Appendix)

| Potential Stakeholders | Potential Stakeholder Contributions |
|--|---|
| Executive Sponsors <ul style="list-style-type: none"> CEO CIO CTO Chief information security officer (CISO) CFO Chief data and analytics officer (CDAO) CHRO | <ul style="list-style-type: none"> Strategize and communicate the cloud-native objectives and how they align with business goals. Help accelerate enterprise performance by focusing on people – through training, organizational structure and governance. Allocate resources and prioritize investments aligned with strategic goals. |
| Cloud, Platform and Solution Architects | <ul style="list-style-type: none"> Responsible for working with the business and technology teams to design cloud architecture and services that support the organization's strategy. |
| Software Engineering Teams | <ul style="list-style-type: none"> Responsible for building cloud-native applications. |
| DevOps Engineers | <ul style="list-style-type: none"> Build, deploy and maintain the infrastructure over which cloud-native applications run. |
| Data and Analytics Teams | <ul style="list-style-type: none"> Manage, optimize, oversee and monitor the retrieval, storage and distribution of data on the cloud. |
| Cloud Operations Engineers | <ul style="list-style-type: none"> Manage and automate secure monitoring of cloud infrastructure. |
| Enterprise Architects | <ul style="list-style-type: none"> Guide the business-led architectural decisions that influence the cloud-native strategy. Ensure compliance with principles, standards and reference architectures. |
| Business Architects | <ul style="list-style-type: none"> Facilitate the design of the future-state business model, its capabilities and roadmap to meet business strategy. Understand the value of existing systems to the business (e.g., from a risk, compliance or business value perspective). |
| Strategic Portfolio Managers | <ul style="list-style-type: none"> Assess the overall portfolio of products, services, programs and projects and ensure compliance and prioritization of resources and funding. Continuously assess benefits versus investments of cloud-native initiatives. Provide project management office support to coordinate the actual realization of the strategy. |
| Legal and Compliance | <ul style="list-style-type: none"> Ensure services are relevant, secure and transparent to others. Provide knowledge about business processes or regulatory requirements. |
| Internal End Users | <ul style="list-style-type: none"> Test and audit services before they are moved to the cloud. |
| Ecosystem Stakeholders <ul style="list-style-type: none"> Cloud Service Provider Regulators Standards Bodies Customers Strategic Vendors Peers at Other Organizations | <ul style="list-style-type: none"> Shape operational best practices in consideration of end users and customers. Ensure compliance to laws and regulations governing security, data sharing and access and identity management. Assist with infrastructure development, ensuring cloud-native applications enable collaboration among ecosystem partners. |

Source: Gartner (October 2022)

Source: Gartner (October 2022)

Our Advice

Refer to [How to Deploy a Cloud Center of Excellence](#) and [Ignition Guide to Building a Cloud Center of Excellence](#) for more information on how executive leaders plan for successful execution of their organizations' cloud strategies.

1.2: Identify business objectives and develop measurable KPIs for cloud-native.

ESSENTIAL

Enterprise leaders should work with stakeholders to identify and agree on which objectives to prioritize and to educate stakeholders on how to leverage cloud-native capabilities to meet those objectives. Keep end users in mind during strategy and implementation design to ensure cloud-native applications and services are accessible and intuitive. Align KPIs to the business objectives identified in the cloud-native strategy, then set a measurement cadence that aligns with the implementation plan. Remember to include technical, business and cultural measures (see Table 2) .

Table 2: Potential Business Objectives, End-User Needs and KPIs

(Enlarged table in Appendix)

| Potential Business Objectives | Potential End-User Needs | Potential KPIs |
|---|---|--|
| <ul style="list-style-type: none"> ■ Reduce costs ■ Enable business continuity ■ Increase speed of development ■ Enable adaptability to changing market conditions ■ Expand revenue opportunities and reduce operational costs ■ Enhance resilience against errors and outages ■ Enable scalability of applications and services ■ Reduce dependency on physical hardware | <ul style="list-style-type: none"> ■ Secure access to data and analytics capabilities ■ Improved productivity through automated tools and services ■ Collaboration with coworkers, external partners and other stakeholders ■ Increased ability to swiftly serve evolving client and customer needs ■ Minimal time and administrative burdens required to develop new applications | <ul style="list-style-type: none"> ■ Cost per user (\$) ■ Cloud spend as a percentage of revenue (%) ■ Reduction in cost of goods sold over time (%) ■ Cost of revenue over time (\$) ■ Time to bring new services to market (time) ■ Compliance issues open (n) ■ Customer satisfaction (typically using Net Promoter Score) ■ Service availability (uptime) (%) ■ Alignment to business roadmap (%) ■ Productivity improvement (%) ■ Number of users with access to services (n) ■ Effective cost per resource (i.e., \$/compute hour) (\$) ■ Security incidents per month (n) ■ Security vulnerabilities identified per month (n) ■ Services automated (%) |

Source: Gartner (October 2022)

1.3: Use business objectives to enhance cloud-native benefits.

Some of the key benefits to becoming cloud-native include increased elasticity, resilience, speed of development, accessibility, analytical power and cost efficiency. A cloud-native strategy should be designed to optimize these benefits in tandem with business objectives (see Figure 3).

Table 3: Benefits of Cloud-Native Design

| Benefit ↓ | Definition ↓ |
|----------------------|--|
| Elasticity | Elasticity helps system users prevent overprovisioning or underprovisioning cloud resources. Overprovisioning refers to a scenario where you buy more capacity than you need. Underprovisioning refers to allocating fewer resources than you use. |
| Resilience | Resiliency is the process of foreseeing possible disruptions to cloud services. It involves planning for business continuity, as well as how the cloud systems will recover with speed and without data loss. |
| Speed of Development | The business agility and momentum that is the result of being able to deploy daily in the cloud, rather than monthly or at even longer intervals, means new products and services can get to market faster. |
| Accessibility | When using cloud-native services, employees, partners and customers can access and update information from any location. Those updates are cascaded automatically, or in near real time. |
| Cost Efficiency | There are many pay-as-you-go packages and other scalable options available for cloud-native services that make it reasonable for businesses of any size to switch from traditional on-premises hardware to the cloud. |
| | |

Our Advice

Identify stakeholder priorities in advance to ensure that development and implementation teams devote time and resources appropriately.

Step 2 of 4: Develop the Strategy

A documented strategy is essential to achieving mission-critical priorities and streamlining implementation. Key elements of the cloud-native strategy include:

- Clear articulation of cloud-native principles (as defined by the enterprise).
- Outline of business objectives.
- Illustration of how cloud-native will enhance the organization's ability to meet those objectives.
- Outline of how success will be defined and measured.
- Well-defined exit strategy.

Tasks








2.1: Complete a comprehensive needs assessment for cloud-native. **ESSENTIAL**

A comprehensive needs assessment for cloud-native should address technical and change management considerations. Ensure security, risk and compliance issues are addressed upfront to reduce potential for business disruption that wastes time, effort and resources (see Figure 3).

Figure 3. Readiness Considerations for Your Cloud-Native Strategy

Readiness Considerations for Your Cloud-Native Strategy

Assess Enterprise Readiness Across Each of These Seven Domains

| Technical Considerations | Change Management Considerations |
|--|---|
|  Storage <ul style="list-style-type: none"> • What are my storage needs/capabilities? |  Talent <ul style="list-style-type: none"> • Do I have a team to implement my strategy? • How will I ensure downstream users have the right skills? |
|  Security <ul style="list-style-type: none"> • How can cloud-native improve existing security? |  Customer/User Experience <ul style="list-style-type: none"> • What access and identity management infrastructure should I design (Who needs access? How often?)? • Will the organization see usage surges/disruptions? |
|  Applications <ul style="list-style-type: none"> • What applications must be rearchitected? • Which applications should I prioritize in my strategy? |  Culture of Innovation <ul style="list-style-type: none"> • How can I use a cloud-native strategy to enable all members of my team to innovate? |
|  Deployment and Provider Services <ul style="list-style-type: none"> • How elastic and portable is my existing infrastructure? | |

Source: Gartner
778541_C

Gartner

Our Advice

Refer to the [Infographic: Cloud Strategy Cookbook](#) for recommendations on how to design a cloud strategy document to share with the organization. A cloud strategy document answers the “what and why” questions, whereas an implementation plan answers the “how” questions. A cloud strategy is a “concise viewpoint on the role of cloud computing in an organization.”

2.2: Manage risk by defining an exit strategy.

A cloud exit strategy ensures that cloud services that support business activities can be substituted without significant disruption to business operations. A cloud exit strategy helps:

- Maintain business continuity and reliability.
- Adapt efficiently to changing market conditions.

- Respond to compliance, regulation and legal requirements without compromising business continuity.
- Overcome pressures of vendor lock-in.

Table 4: Considerations When Planning a Cloud Exit Strategy

(Enlarged table in Appendix)

| Considerations ↓ | Actions ↓ |
|--|---|
| Terms & conditions and SLAs | Be able to meet all contractual agreements until your cloud exit is complete. |
| Data ownership, backup and data recovery | Ensure that the data format meets portability requirements. |
| Lock-in | Consider lock-in at the data level, the application level, the architecture level or the skills level. |
| Type of service | When you consider SaaS vendors, take into account that many vendors are becoming pure-play SaaS providers. Fewer traditional on-premises offerings are available. |
| Development and architectural issues | Ensure that your cloud architecture allows data and applications to be portable. |
| Multicloud strategies | Consider using a combination of clouds – which can be two or more public, private and/or edge clouds – to reduce dependency on a single vendor. |
| Strategy, not a detailed plan | Focus your exit strategy on answering “what?” and “why?” questions. |
| Implementation | Cover the answers to “how?” questions in a more detailed exit plan. |

Source: Gartner (October 2022)

2.3: Communicate cloud-native architectural principles to decision makers.

Cloud-native architectural principles are the set of application architecture principles and design patterns that enable applications to fully utilize the capabilities provided by cloud computing. Cloud-native applications are architected to be latency-aware, instrumented, failure-aware, event-driven, secure, parallelizable, automated, and resource-consumption-aware. Architecture principles and considerations are key to successful deployments of cloud-native services. These principles are outlined in Gartner’s LIFESPAR framework (see Table 5).

Table 5: Architectural Principles for Cloud-Native (LIFESPAR)

(Enlarged table in Appendix)

| <i>Principle</i> ↓ | <i>Impact</i> ↓ |
|----------------------------|--|
| Latency-aware | Applications remain operational despite variable and extended latency for services accessed across public networks, and between cloud provider data centers. |
| Instrumented | Sufficient telemetry data is available from applications to determine health and other operational and performance characteristics. |
| Failure-aware | Applications are resilient to occasional or extended failures of underlying infrastructure components or dependent services. |
| Event-driven | Programs are structured as a set of handlers, waiting for events and responding in a choreographed way – rather than with sequential, determined and synchronous orchestrations. |
| Secure | The application protects the information and systems, guarding against data loss or SLA violations caused by malicious or accidental events. |
| Parallelizable | Data processing can be scaled out to multiple simultaneous or redundant instances of system components. |
| Automated | Applications are packaged, deployed and executed without manual steps or complex dependencies. |
| Resource-consumption-aware | Applications can be adapted to different algorithms, data structures and system architecture in response to resource cost changes. |

Source: Gartner (October 2022)

Source: Gartner (October 2022)

Our Advice

Refer to [A CTO's Guide to Cloud-Native: Answering the Top 10 FAQs](#) for answers to the most common questions related to the multiple uses of cloud-native that will guide enterprise leaders to make sound decisions.

Step 3 of 4: Implement the Strategy

An implementation plan helps define the “how” of the cloud-native journey, establishes the pace of deployment, assigns deployment responsibilities and ensures streamlined deployment among stakeholders. The implementation phase can be thought of as putting the strategy document into practice, where deadlines, resources and responsible parties are identified.

Tasks

3.1: Create an implementation roadmap.

Use the results of the needs assessment (outlined in step 2.1) to create an implementation roadmap using a phased approach that aligns efforts and resources with desired business outcomes. Starting with an MVP approach significantly lowers the risk of commercial mistakes, such as investing a large sum of money in the wrong idea or running over budget (see tool below).

[Tool: Cloud-Native Implementation Roadmap](#)

3.2: Overcome common obstacles.

The complexities of operating in a cloud-native environment can be overwhelming, because of the growing number of competing technologies and resulting architectural complexity. Enterprise leaders should proactively identify and address the obstacles to effective design and delivery of cloud-native services (see Table 6).

Table 6: Common Obstacles to Implementing Cloud-Native Services

(Enlarged table in Appendix)

| Obstacle ↓ | Why the Obstacle Is Important ↓ | How to Overcome (suggested) ↓ |
|--------------------------------|--|---|
| Data Handling and Storage | Cloud-native systems store data externally, as opposed to traditional applications, where data is typically stored internally. Cloud service providers often offer data encryption/decryption and management as part of the storage service; enterprises will need to evaluate whether these data management services meet usage needs and compliance regulations. | Developers need to redefine their data storage, identity management and access strategies, which requires additional effort in the planning stage and will require automated monitoring mechanisms throughout the life cycle. |
| Vendor Lock-In | Switching vendors at a later stage of deployment results in high operational costs, operational disruptions, architectural complexity and steep overhead. | To build scalable applications and maximize cloud-native benefits, individuals tasked with selecting and managing vendor relationships need to minimize lock-in risk by planning well ahead and defining an exit strategy that addresses resulting trade-offs. |
| Security and Compliance Issues | Organizations will need to consider how to grant access to cloud-native storage and applications, how to effectively monitor access and how to educate all stakeholders on maintaining security and preventing data breaches. | Organizations should prioritize developing their cloud-native infrastructure in alignment with security requirements and compliance regulations. |
| Lack of Technical Expertise | Finding skilled IT cloud talent is a difficult task for most organizations. Some companies are forced to slow the process of moving to cloud-native due to talent shortages or absence of an internal upskilling plan. | Companies should focus on developing a plan to source new talent and regularly train new hires and existing employees on emerging cloud-native capabilities. |
| Use of Outdated Technologies | It is crucial to keep up with the latest developments in cloud technologies and find their cloud-native equivalents. The use of outdated technologies results in low-quality, inefficient applications and slows down the business. | A portion of the cloud-native implementation team should be devoted to trendspotting and establishing proofs of concept for emerging capabilities. |
| Complex Cloud-Native Concepts | Stakeholders with limited IT expertise can be overwhelmed by technical decisions associated with cloud-native adoption. Understanding the core concepts of cloud-native like microservices, serverless computing, and containers can be challenging without the help of a cloud expert. | Cloud architects should play a role in educating stakeholders about fundamental cloud concepts and technology; cloud architects, and other IT leaders, should facilitate internal upskilling efforts to ensure that they are able to seamlessly leverage emerging services. |

Source: Gartner (October 2022)

Our Advice

Refer to [Quick Answer: How Do I Overcome a Lack of Cloud Skills in My Organization?](#) and [How to Overcome Resistance to Cloud Adoption in an I&O Team](#) for more information on how to accelerate skills development and to encourage adoption of cloud technologies.

3.3: Proactively address change management. **ESSENTIAL**

Managing changes to capabilities, requirements and ways of working requires a human-centric approach. Additions to, and the modification or removal of, legacy applications or systems will have direct or indirect impacts on how the business delivers products and services. Address technological, organizational and cultural changes to ensure the implementation plan is executed effectively (see Table 7).

Table 7: Potential Changes to Capabilities, Requirements and Ways of Working

(Enlarged table in Appendix)

| Type of Change ↓ | Implications of Change ↓ |
|------------------------|--|
| Technological changes | <ul style="list-style-type: none"> ■ New tools for containerization, orchestration, continuous integration/deployment and other cloud-native requirements. ■ Teams will also need to change the way they build applications to favor microservices, which may require additional training and/or technology. |
| Organizational changes | <ul style="list-style-type: none"> ■ Before, enterprises were building on-premises or building until complete, then delivering. Now, enterprises need to create minimum viable products and build solutions incrementally. ■ Cloud-native requires all teams to focus on collaboration, allowing the enterprise to shrink the feedback loop between developers and end users and ensure that code can be delivered, tested and fixed as quickly as possible. |
| Cultural changes | <ul style="list-style-type: none"> ■ Cloud-native often includes the support of agile and DevOps methodologies, which require a cultural shift. ■ Collaboration should be the No. 1 priority for navigating cultural changes, with everyone committing to breaking down silos that keep developers, testers and others from working together effectively. |

Source: Gartner (October 2022)

Step 4 of 4: Measure Performance and Make Improvements

Shifting systems to be cloud-native is not a singular activity. Cloud-native applications and services require iterative development and maintenance to maximize their utility. Be wary of transitioning to cloud-native too fast and assuming that there is a clearly specified end destination.

Tasks

4.1: Monitor operational performance.

Create processes to monitor and measure the performance of cloud-native systems. Use the Cloud-Native Implementation Roadmap (outlined in step 3.1) to assess whether you are meeting implementation goals effectively.

Cloud monitoring efforts should include end-user feedback, which will require feedback mechanisms that end users can access to improve services and enable greater autonomy. Potential feedback mechanisms include:

- Dashboards that help users act on critical business opportunities on demand, with the most up-to-date data.
- Internal surveys that give users the ability to provide annotated feedback.
- Foundational training for those who don't have experience working with cloud-native services.
- End-user journey mapping that helps decision makers proactively identify bottlenecks and obstacles.
- Opportunities for users to collaborate and share critical insights with minimal assistance from IT.

Our Advice

The cloud monitoring process should extend beyond the initial implementation period and incorporate KPIs identified in the cloud-native strategy.

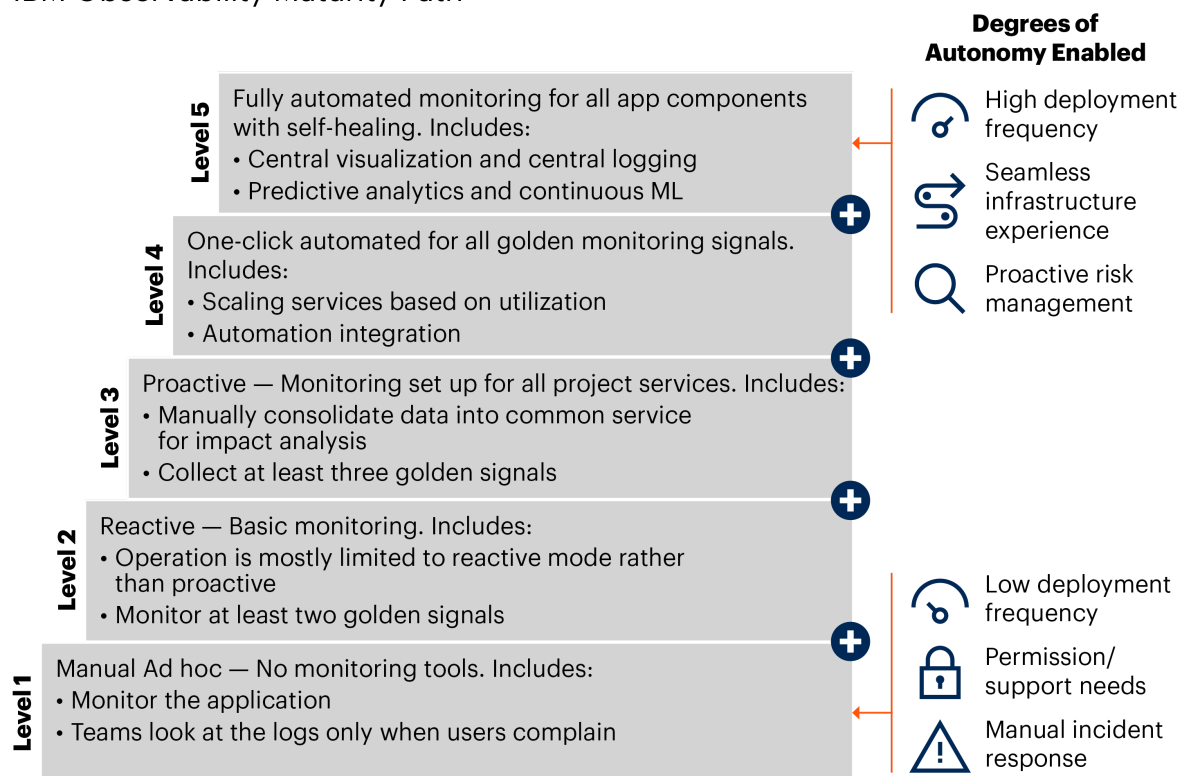
4.2: Establish guardrails and automated protocols. **ESSENTIAL**

Though increased accessibility and accelerated development are key benefits of cloud-native services, they come with associated risks that should be addressed during implementation. Trigger-based automated guardrails, protocols and development standards help ensure risks are mitigated and architectural complexity is kept to a minimum (see Figure 4).

Figure 4. Link Monitoring With Application Team Objectives

Link Monitoring With Application Team Objectives

IBM Observability Maturity Path



Source: Adapted From IBM

760101_C

Gartner

Review Your Performance

- Discuss cloud-native as an approach that enables business outcomes to be met, rather than focusing on the technicalities of what cloud-native can do.
- Reassess the cloud-native strategy as your enterprise strategy evolves and consider execution of the “exit” strategy in case business objectives are not being met (see step 2.2).
- Reevaluate your cloud-native resources and vendor relationships to ensure that you work with the ones that have the most up-to-date technologies and resources.
- Monitor and manage cost and resource use, ensure adherence to security and compliance requirements and mitigate architectural complexity that can come from accelerated cloud-native transformation.

Recommended by the Authors

[Top Strategic Technology Trends for 2022: Cloud-Native Platforms](#)

[A CTO's Guide to Cloud-Native: Answering the Top 10 FAQs](#)

[Infographic: Cloud Strategy Cookbook](#)

[Hype Cycle for Cloud Computing, 2022](#)

[How to Navigate the Application Platforms Market Including Cloud-Native, Low-Code, and SaaS](#)

[The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem](#)

[Quick Answer: How Do I Overcome a Lack of Cloud Skills in My Organization?](#)

[Case Study: Optimize Monitoring for a Dynamic Application Portfolio \(IBM\)](#)

Disclaimer: Please note because there are many items in the Ignition Guide, you will see this disclaimer only once, but it is intended to apply to all items in the guide. Unless otherwise set forth in your Service Description or marked expressly for external use, these items may be downloaded and customized for internal noncommercial use by the Client. The items may not be repackaged or resold. Gartner makes no representations or warranties as to the suitability of these items for any particular purpose, and disclaims all liability for any damage or loss, whether direct, consequential, incidental or special, arising out of the use of or inability to use this material or the information provided herein.

Spreadsheets published by Gartner may leverage features such as pivot tables and macros that are supported in a Microsoft Windows environment and with Microsoft Excel 2007 or higher.

See Gartner Internet Browser [System Requirements](#) for more information.

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

1. [Align cloud-native strategy to business objectives.](#)
2. [Develop the strategy.](#)
3. [Implement the strategy.](#)
4. [Measure performance and make improvements.](#)

| Common Pitfalls | Keys to Success |
|--|---|
| All-or-Nothing Approach Enterprise leaders struggle to determine which applications and assets need to be run in the cloud and which do not, defaulting to the philosophy that they either all need to be cloud-based or not. | Focus on Generating Incremental Value Early Invest as you scale rather than deliver a large investment upfront. Starting with a narrow, well-defined use case first helps evaluate whether it will generate the intended business outcome, gauge talent and technical issues and plan for future scalability. |
| Insufficient Understanding of Intended Value and Anticipated Costs Lots of hype and technicalities exist around cloud-native, which makes it difficult to understand what cloud-native is, how much it will cost and how it can be used to provide return on investment. | Implement Monitoring and Diagnostics From the Start Prior to adoption, establish mechanisms to monitor and assess usage of cloud resources and total expense to align cloud-native strategy to business objectives and to ensure sufficient understanding of intended value. |
| Failing to Consider Organizational Nuances There is no single tool, delivery model or vendor that is appropriate for all organizational contexts; while some tools, delivery models and/or vendors might have worked for other organizations, mimicking those may not solve your enterprise's business objectives. | Actively Meet Organization-Specific Demands Placed on Cloud-Native Systems Continually conduct capabilities and requirements analysis to discern the right approach to achieving your intended outcomes. |
| Not Planning for Cultural Change Considering cloud-native as an "IT only" initiative focuses solely on the technical perspective, which could lead to resistance from business partners that can delay progress. | Engage All Relevant Stakeholders to Communicate Objectives and Potential Disruptions Stakeholders must have clear visibility of changes to ways of working and must have a chance to articulate needs or requirements directly. |
| Overdependence on a Platform or Provider's Security Services Cloud service providers may not always provide the right array of capabilities and services that the enterprise needs, particularly when it comes to security. Committing to a single provider prematurely could lock the enterprise into | Implement Security Across the Entire Life Cycle of an Application From design and implementation to deployment and operations, focus on identity management, infrastructure access, application security and data sovereignty and encryption. Assess potential providers and capabilities and |

capabilities and services ill-suited to business objectives or compliance restrictions.

look for multivendor strategies, as long as these meet business and technology expectations.

Table 1: List of Potential Stakeholders to Consult

| Potential Stakeholders ↓ | Potential Stakeholder Contributions ↓ |
|--|--|
| Executive Sponsors <ul style="list-style-type: none"> ■ CEO ■ CIO ■ CTO ■ Chief information security officer (CISO) ■ CFO ■ Chief data and analytics officer (CDAO) ■ CHRO | <ul style="list-style-type: none"> ■ Strategize and communicate the cloud-native objectives and how they align with business goals. ■ Help accelerate enterprise performance by focusing on people — through training, organizational structure and governance. ■ Allocate resources and prioritize investments aligned with strategic goals. |
| Cloud, Platform and Solution Architects | <ul style="list-style-type: none"> ■ Responsible for working with the business and technology teams to design cloud architecture and services that support the organization's strategy. |
| Software Engineering Teams | <ul style="list-style-type: none"> ■ Responsible for building cloud-native applications. |

| Potential Stakeholders ↓ | Potential Stakeholder Contributions ↓ |
|----------------------------|--|
| DevOps Engineers | <ul style="list-style-type: none"> ■ Build, deploy and maintain the infrastructure over which cloud-native applications run. |
| Data and Analytics Teams | <ul style="list-style-type: none"> ■ Manage, optimize, oversee and monitor the retrieval, storage and distribution of data on the cloud. |
| Cloud Operations Engineers | <ul style="list-style-type: none"> ■ Manage and automate secure monitoring of cloud infrastructure. |
| Enterprise Architects | <ul style="list-style-type: none"> ■ Guide the business-led architectural decisions that influence the cloud-native strategy. ■ Ensure compliance with principles, standards and reference architectures. |
| Business Architects | <ul style="list-style-type: none"> ■ Facilitate the design of the future-state business model, its capabilities and roadmap to meet business strategy. ■ Understand the value of existing systems to the business (e.g., from a risk, compliance or business value perspective). |

| <i>Potential Stakeholders</i> ↓ | <i>Potential Stakeholder Contributions</i> ↓ |
|---------------------------------|---|
| Strategic Portfolio Managers | <ul style="list-style-type: none"> ■ Assess the overall portfolio of products, services, programs and projects and ensure compliance and prioritization of resources and funding. ■ Continuously assess benefits versus investments of cloud-native initiatives. ■ Provide project management office support to coordinate the actual realization of the strategy. |
| Legal and Compliance | <ul style="list-style-type: none"> ■ Ensure services are relevant, secure and transparent to others. ■ Provide knowledge about business processes or regulatory requirements. |
| Internal End Users | <ul style="list-style-type: none"> ■ Test and audit services before they are moved to the cloud. |
| | |

| Potential Stakeholders ↓ | Potential Stakeholder Contributions ↓ |
|--|--|
| Ecosystem Stakeholders <ul style="list-style-type: none"> ■ Cloud Service Provider ■ Regulators ■ Standards Bodies ■ Customers ■ Strategic Vendors ■ Peers at Other Organizations | <ul style="list-style-type: none"> ■ Shape operational best practices in consideration of end users and customers. ■ Ensure compliance to laws and regulations governing security, data sharing and access and identity management. ■ Assist with infrastructure development, ensuring cloud-native applications enable collaboration among ecosystem partners. |

Source: Gartner (October 2022)

Table 2: Potential Business Objectives, End-User Needs and KPIs

| Potential Business Objectives | Potential End-User Needs | Potential KPIs |
|---|---|--|
| <ul style="list-style-type: none"> ■ Reduce costs ■ Enable business continuity ■ Increase speed of development ■ Enable adaptability to changing market conditions ■ Expand revenue opportunities and reduce operational costs ■ Enhance resilience against errors and outages ■ Enable scalability of applications and services ■ Reduce dependency on physical hardware | <ul style="list-style-type: none"> ■ Secure access to data and analytics capabilities ■ Improved productivity through automated tools and services ■ Collaboration with coworkers, external partners and other stakeholders ■ Increased ability to swiftly serve evolving client and customer needs ■ Minimal time and administrative burdens required to develop new applications | <ul style="list-style-type: none"> ■ Cost per user (\$) ■ Cloud spend as a percentage of revenue (%) ■ Reduction in cost of goods sold over time (%) ■ Cost of revenue over time (\$) ■ Time to bring new services to market (time) ■ Compliance issues open (n) ■ Customer satisfaction (typically using Net Promoter Score) ■ Service availability (uptime) (%) ■ Alignment to business roadmap (%) ■ Productivity improvement (%) ■ Number of users with access to services (n) ■ Effective cost per resource (i.e., \$/compute hour) (\$) ■ Security incidents per month (n) ■ Security vulnerabilities identified per month (n) ■ Services automated (%) |

Source: Gartner (October 2022)

Table 3: Benefits of Cloud-Native Design

| <i>Benefit</i> ↓ | <i>Definition</i> ↓ |
|----------------------|--|
| Elasticity | Elasticity helps system users prevent overprovisioning or underprovisioning cloud resources. Overprovisioning refers to a scenario where you buy more capacity than you need. Underprovisioning refers to allocating fewer resources than you use. |
| Resilience | Resiliency is the process of foreseeing possible disruptions to cloud services. It involves planning for business continuity, as well as how the cloud systems will recover with speed and without data loss. |
| Speed of Development | The business agility and momentum that is the result of being able to deploy daily in the cloud, rather than monthly or at even longer intervals, means new products and services can get to market faster. |
| Accessibility | When using cloud-native services, employees, partners and customers can access and update information from any location. Those updates are cascaded automatically, or in near real time. |
| Cost Efficiency | There are many pay-as-you-go packages and other scalable options available for cloud-native services that make it reasonable for businesses of any size to switch from traditional on-premises hardware to the cloud. |

Source: Gartner (October 2022)

Table 4: Considerations When Planning a Cloud Exit Strategy

| Considerations ↓ | Actions ↓ |
|--|---|
| Terms & conditions and SLAs | Be able to meet all contractual agreements until your cloud exit is complete. |
| Data ownership, backup and data recovery | Ensure that the data format meets portability requirements. |
| Lock-in | Consider lock-in at the data level, the application level, the architecture level or the skills level. |
| Type of service | When you consider SaaS vendors, take into account that many vendors are becoming pure-play SaaS providers. Fewer traditional on-premises offerings are available. |
| Development and architectural issues | Ensure that your cloud architecture allows data and applications to be portable. |
| Multicloud strategies | Consider using a combination of clouds – which can be two or more public, private and/or edge clouds – to reduce dependency on a single vendor. |
| Strategy, not a detailed plan | Focus your exit strategy on answering “what?” and “why?” questions. |
| Implementation | Cover the answers to “how?” questions in a more detailed exit plan. |

Source: Gartner (October 2022)

Table 5: Architectural Principles for Cloud-Native (LIFESPAR)

| Principle ↓ | Impact ↓ |
|----------------------------|--|
| Latency-aware | Applications remain operational despite variable and extended latency for services accessed across public networks, and between cloud provider data centers. |
| Instrumented | Sufficient telemetry data is available from applications to determine health and other operational and performance characteristics. |
| Failure-aware | Applications are resilient to occasional or extended failures of underlying infrastructure components or dependent services. |
| Event-driven | Programs are structured as a set of handlers, waiting for events and responding in a choreographed way – rather than with sequential, determined and synchronous orchestrations. |
| Secure | The application protects the information and systems, guarding against data loss or SLA violations caused by malicious or accidental events. |
| Parallelizable | Data processing can be scaled out to multiple simultaneous or redundant instances of system components. |
| Automated | Applications are packaged, deployed and executed without manual steps or complex dependencies. |
| Resource-consumption-aware | Applications can be adapted to different algorithms, data structures and system architecture in response to resource cost changes. |

Source: Gartner (October 2022)

Table 6: Common Obstacles to Implementing Cloud-Native Services

| <i>Obstacle</i> ↓ | <i>Why the Obstacle Is Important</i> ↓ | <i>How to Overcome (suggested)</i> ↓ |
|--------------------------------|--|--|
| Data Handling and Storage | Cloud-native systems store data externally, as opposed to traditional applications, where data is typically stored internally. Cloud service providers often offer data encryption/decryption and management as part of the storage service; enterprises will need to evaluate whether these data management services meet usage needs and compliance regulations. | Developers need to redefine their data storage, identity management and access strategies, which requires additional effort in the planning stage and will require automated monitoring mechanisms throughout the life cycle. |
| Vendor Lock-In | Switching vendors at a later stage of deployment results in high operational costs, operational disruptions, architectural complexity and steep overhead. | To build scalable applications and maximize cloud-native benefits, individuals tasked with selecting and managing vendor relationships need to minimize lock-in risk by planning well ahead and defining an exit strategy that addresses resulting trade-offs. |
| Security and Compliance Issues | Organizations will need to consider how to grant access to cloud-native storage and applications, how to effectively monitor access and how to educate all stakeholders on maintaining security and preventing data breaches. | Organizations should prioritize developing their cloud-native infrastructure in alignment with security requirements and compliance regulations. |

| <i>Obstacle</i> ↓ | <i>Why the Obstacle Is Important</i> ↓ | <i>How to Overcome (suggested)</i> ↓ |
|-------------------------------|---|---|
| Lack of Technical Expertise | Finding skilled IT cloud talent is a difficult task for most organizations. Some companies are forced to slow the process of moving to cloud-native due to talent shortages or absence of an internal upskilling plan. | Companies should focus on developing a plan to source new talent and regularly train new hires and existing employees on emerging cloud-native capabilities. |
| Use of Outdated Technologies | It is crucial to keep up with the latest developments in cloud technologies and find their cloud-native equivalents. The use of outdated technologies results in low-quality, inefficient applications and slows down the business. | A portion of the cloud-native implementation team should be devoted to trendspotting and establishing proofs of concept for emerging capabilities. |
| Complex Cloud-Native Concepts | Stakeholders with limited IT expertise can be overwhelmed by technical decisions associated with cloud-native adoption. Understanding the core concepts of cloud-native like microservices, serverless computing, and containers can be challenging without the help of a cloud expert. | Cloud architects should play a role in educating stakeholders about fundamental cloud concepts and technology; cloud architects, and other IT leaders, should facilitate internal upskilling efforts to ensure that they are able to seamlessly leverage emerging services. |

Source: Gartner (October 2022)

Table 7: Potential Changes to Capabilities, Requirements and Ways of Working

| Type of Change ↓ | Implications of Change ↓ |
|------------------------|---|
| Technological changes | <ul style="list-style-type: none">■ New tools for containerization, orchestration, continuous integration/deployment and other cloud-native requirements.■ Teams will also need to change the way they build applications to favor microservices, which may require additional training and/or technology. |
| Organizational changes | <ul style="list-style-type: none">■ Before, enterprises were building on-premises or building until complete, then delivering. Now, enterprises need to create minimum viable products and build solutions incrementally.■ Cloud-native requires all teams to focus on collaboration, allowing the enterprise to shrink the feedback loop between developers and end users and ensure that code can be delivered, tested and fixed as quickly as possible. |
| Cultural changes | <ul style="list-style-type: none">■ Cloud-native often includes the support of agile and DevOps methodologies, which require a cultural shift.■ Collaboration should be the No. 1 priority for navigating cultural changes, with everyone committing to breaking down silos that keep developers, testers and others from working together effectively. |

Type of Change ↓

Implications of Change ↓

Source: Gartner (October 2022)