IT Efficiency Index Powered by Intellyx

How to Modernize Your Approach to Infrastructure Monitoring

MONITORING MATURITY MODEL FOR THE DIGITAL ERA

WHY DO WE NEED AN IT MATURITY MODEL?

The entire enterprise IT infrastructure landscape is undergoing an end-to-end transformation. Cloud computing is now a must-have – and enterprises want more than one, combining public and private clouds with on-premises environments into an abstracted hybrid IT landscape.

Meanwhile, each environment hosts a cocktail of technologies, from virtualization to containers to serverless computing. As this complex, dynamic IT infrastructure evolves, systems and services are becoming more distributed, people and processes change, and the probability of service outages increases.

As a result, hybrid infrastructure performance monitoring is an essential tool. It offsets the inherent complexity of modern hybrid IT environments by providing unified performance data and visibility across applications and infrastructure, on-premises and in one or more clouds.

THE ROLE OF THE MATURITY MODEL

Enterprise operations teams already have a plethora of monitoring tools, most or all of which aren't up to the challenge of this new digital era. How can teams embrace the chaos of today's fast-paced and constantly scaling environments without first assessing their current status?

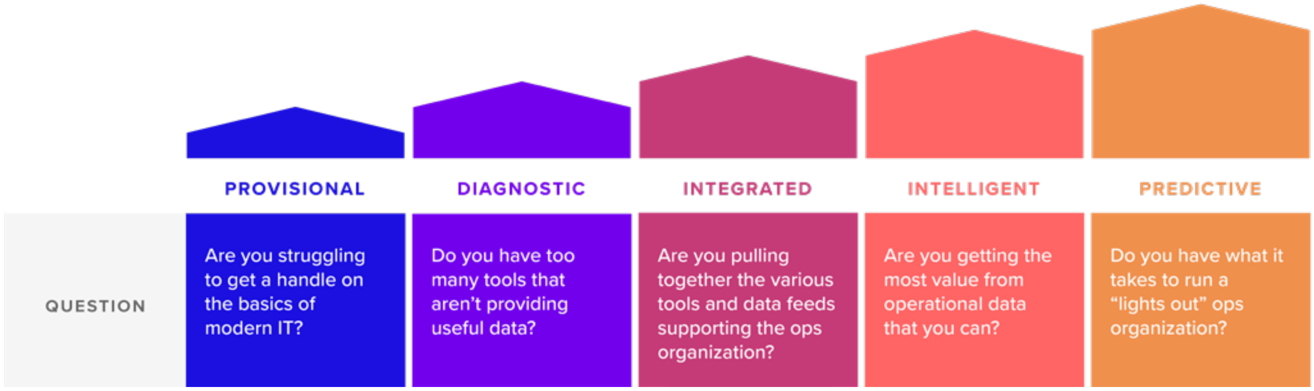
	PROVISIONAL	DIAGNOSTIC	INTEGRATED	INTELLIGENT	PREDICTIVE
CLOUD AGILITY	**Fully On-premises** Pre-cloud state.	**Discrete Cloud Uses** Early cloud use consists of individual SaaS services and limited IaaS use.	**Simple Cloud Integration/VPC** IT extends internal environment to the cloud.	**Early Hybrid/Multicloud** Multiple cloud deployments and complex virtualization scenarios lead to a hybrid IT strategy.	**Fully Hybrid** Deployment options fully abstracted. Focus is o business value of qorkoads that support customer-facing apps and services.
ARCHITECTURE	**Client Server/ Monolithic Applications** Centralized, on-premises architectures.	**Virtualization-supported** On-premises virtualization expands options for IT.	**SOA/Scale Out/Elasticity** Cloud architectures extend on-premises IT and also open up new possibilities for on-prem and hybrid architectures.	**Containers/ Microservices Architecture** Containerization capitalizes on cloud architecture best practices to drive greater agility & business velocity. Microservices architecture leverages the power and flexibility of containers.	**Serverless/ Next-gen Architectures** Next-gen architectures are largely undefined. Serverless computing gives us a taste of what's to come.
SOFTWARE DEVELOPMENT	**Waterfall/ Limited Agile** Early Agile attempts have improved waterfall to a certain extent, but waterfall mentality still dominates.	**Agile** Agile becomes the default across the organization, but teams struggle with its shortcomings.	**DevOps** As ops becomes more automated, organizations undergo the cultural DevOps shift to greater collaboration and empathy, driving increased business velocity.	**DevSecOps** DevOps extends beyond dev and ops, first to security and quality, but eventually to product and marketing teams as well.	**Scaled DevSecOps** The DevOps cultural shift expands across the organization as part of its broad horizontal reorganization.
DIGITAL TRANSFORMATION	**Websites & Mobile Apps** Starting point for digital transformation includes various online efforts.	**Customer Journey** Enterprises realign efforts to better meet the needs of customers when and where they wish to interact with the companies they do business with.	**End-to-end Customer Focus** Customer journey focus extends from systems of engagement to systems of record, bringing all of IT in alignment with digital priorities.	**Horizontal Reorganization** Org charts flatten and blur as self-organization spearheads transformation efforts. Remaining managers become leaders as they drive decision making down into the organization.	**Change as Core Competency** Change itself becomes a core competency as the entire organization -- people as well as technology -- align with ever-changing customer desires.

Organizations are not linear and IT evolution timelines differ by company and business needs. While there is no guaranteed recipe for an idyllic IT end-state, a maturity model can lay out a framework for progress by taking complex, multidimensional problem areas and compartmentalizing them into a manageable grid, with the end goal of optimized service delivery.

As the chart on the previous page illustrates, we've summarized the challenges facing modern IT organizations into four core dimensions: cloud adoption, architecture, software development, and digital transformation.

MONITORING: ASKING THE RIGHT QUESTIONS

The first step to placing IT monitoring into the context of the maturity model above is to ask the right questions. These questions then suggest the appropriate labels for each level.



	PROVISIONAL	DIAGNOSTIC	INTEGRATED	INTELLIGENT	PREDICTIVE
QUESTION	Are you struggling to get a handle on the basics of modern IT?	Do you have too many tools that aren't providing useful data?	Are you pulling together the various tools and data feeds supporting the ops organization?	Are you getting the most value from operational data that you can?	Do you have what it takes to run a "lights out" ops organization?

At level 1 – pre-cloud, pre-Agile organizations are dealing with data overload and alert fatigue, but lack the proper tools for root cause analysis of the problems they face.

At level 2 – organizations are using a variety of monitoring solutions for different parts of their infrastructure, opening up doors for inevitable chair swivel due to too many tools.

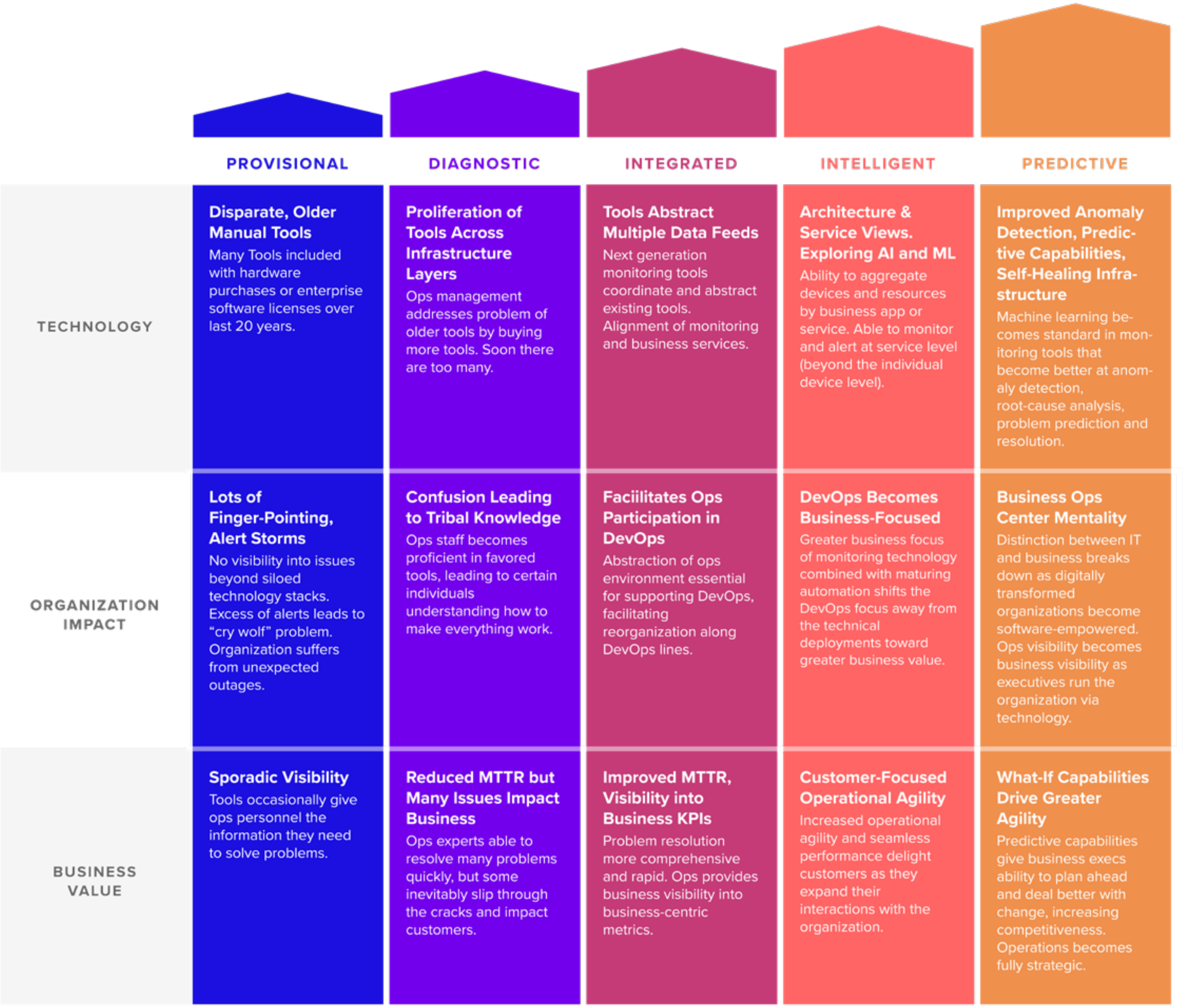
At level 3 – ops personnel are integrating more sophisticated tools, allowing teams to have a more holistic view of the entire infrastructure stack and respond quicker to incidents.

At level 4 – machine learning enters into the mix, enabling organizations to extract maximum value from operational data.

At level 5 – an organization's monitoring becomes sophisticated enough to predict problems before they occur, enabling organizations to operate their IT environment automatically with little to no adverse impact on customers.

THE MONITORING MATURITY MODEL

Within the context of the five levels of this maturity model, there are three core dimensions of IT monitoring: technology, organizational impact, and business value.



	PROVISIONAL	DIAGNOSTIC	INTEGRATED	INTELLIGENT	PREDICTIVE
TECHNOLOGY	**Disparate, Older Manual Tools** Many Tools included with hardware purchases or enterprise software licenses over last 20 years.	**Proliferation of Tools Across Infrastructure Layers** Ops management addresses problem of older tools by buying more tools. Soon there are too many.	**Tools Abstract Multiple Data Feeds** Next generation monitoring tools coordinate and abstract existing tools. Alignment of monitoring and business services.	**Architecture & Service Views. Exploring AI and ML** Ability to aggregate devices and resources by business app or service. Able to monitor and alert at service level (beyond the individual device level).	**Improved Anomaly Detection, Predictive Capabilities, Self-Healing Infrastructure** Machine learning becomes standard in monitoring tools that become better at anomaly detection, root-cause analysis, problem prediction and resolution.
ORGANIZATION IMPACT	**Lots of Finger-Pointing, Alert Storms** No visibility into issues beyond siloed technology stacks. Excess of alerts leads to "cry wolf" problem. Organization suffers from unexpected outages.	**Confusion Leading to Tribal Knowledge** Ops staff becomes proficient in favored tools, leading to certain individuals understanding how to make everything work.	**Faciilitates Ops Participation in DevOps** Abstraction of ops environment essential for supporting DevOps, facilitating reorganization along DevOps lines.	**DevOps Becomes Business-Focused** Greater business focus of monitoring technology combined with maturing automation shifts the DevOps focus away from the technical deployments toward greater business value.	**Business Ops Center Mentality** Distinction between IT and business breaks down as digitally transformed organizations become software-empowered. Ops visibility becomes business visibility as executives run the organization via technology.
BUSINESS VALUE	**Sporadic Visibility** Tools occasionally give ops personnel the information they need to solve problems.	**Reduced MTTR but Many Issues Impact Business** Ops experts able to resolve many problems quickly, but some inevitably slip through the cracks and impact customers.	**Improved MTTR, Visibility into Business KPIs** Problem resolution more comprehensive and rapid. Ops provides business visibility into business-centric metrics.	**Customer-Focused Operational Agility** Increased operational agility and seamless performance delight customers as they expand their interactions with the organization.	**What-If Capabilities Drive Greater Agility** Predictive capabilities give business execs ability to plan ahead and deal better with change, increasing competitiveness. Operations becomes fully strategic.

Level 1: Provisional

At level 1, organizations have disparate, often manual monitoring tools. In many cases, the tools they have inherited came with other purchases – enterprise applications or hardware that has its own limited monitoring built in.

The focus here is on minimizing downtime, but does not offer support for strategic initiatives such as budget justification, asset management, or provide visibility across multiple systems to effectively troubleshoot when issues occur.

Operating at level 1 forces IT staff to troubleshoot with very limited context, usually resulting in downtime that negatively impacts customers and the overall business.

Here are the key changes required to move to level 2:

1. Eliminate as many vendor-provided tools as possible in favor of one or more tools that support multi-vendor environments.
2. Expand individual device monitoring to include broader service level monitoring.
3. Broaden monitoring granularity to allow for more effective problem resolution, historical tracking and predictability.

To support organizations looking to scale into level 2, LogicMonitor provides a growing library including thousands of pre-built monitoring templates. LogicMonitor intelligently finds and queries many types of devices and environments, automatically applying the appropriate monitoring and alerting for your entire infrastructure.

Level 2: Diagnostic

Operations teams respond to the challenges of level 1 by purchasing dedicated monitoring tools. Depending on tool selection, the mean time to resolution (MTTR) for incidents tend to go down as the team can resolve some problems quickly, however the sheer number of tools leads to a separate set of complications.

Using numerous tools, along with their application specific thresholds and data points, frequently lead to finger-pointing sessions between separate component leads.

For example, there is an element of human involvement to consider. No one individual can be an expert on all the tools. As different engineers become proficient in various tools, organizations quickly develop a tribal knowledge problem: the effectiveness of various initiatives starts to depend upon the participation of specific people.

Here are the key changes required to move to level 3:

1. Determine which tools provide the most visibility across different data sets. Common toolsets include infrastructure, log, and application monitoring.
2. Establish thresholds across device groups and services to route alerts to different teams based on severity, device, technology, groups, or even time of day.
3. Begin to implement automation for ticketing systems, proactive resource allocation and failure analysis.

To support organizations looking to scale into level 3, LogicMonitor delivers built-in integrations with service management tools like ServiceNow, communication tools like Slack, or incident notification tools like PagerDuty. By pulling data from chosen toolsets, integrating with LogicMonitor allows for a single source of truth for infrastructure health.

Level 3: Integrated

At the third level, organizations are adopting a DevOps culture to support the growth requirements of the business. With this shift, operations and development teams must leverage better automation tools to foster greater collaboration, faster application deployment and immediate troubleshooting. At this level, it’s imperative to monitor the entire dev pipeline - from code to release.

Organizations at this level are also at a crossover point where they are beginning to see a positive return on investment from their monitoring application. The team is now able to free resources to perform other strategic activities and all parties involved – from executives to engineers – have a clear view into the health of the business via dashboards and reports.

Here are the key steps to move to level 4:

1. Leverage your monitoring tool to show historical data and graph projections. Forecast when alert thresholds will be crossed, allowing for planned growth with no downtime.
2. Implement proactive tracking of event history to allow for analysis of trending failures.
3. Expand your monitoring KPIs to include custom metrics and devices specific to your mission.

To support organizations looking to scale into level 4, LogicMonitor stores two years of performance data, allowing users to meet demanding SLA targets. This performance data also allows users to visualize long term trends and patterns while predicting future trends based on past performance. This piece is crucial for proactive issue diagnosis and budget planning.

Level 4: Intelligent

At the fourth level, organizations leverage agile monitoring tools with machine learning to extract essential insights from large pools of operational data, learning as they go and improving their ability to discern root causes.

Machine learning addresses two core challenges: insights into dynamic operational data, and identification of problems and their solutions across heterogeneous environments. Most organizations at this level have excellent visibility into their entire infrastructure by integrating strategic tools and are able to apply proactive failure analysis.

The benefits of these capabilities are profound. Internally, this proactive resolution has significantly lowered costs, directly impacting the IT teams. Externally, the outcome is nothing less than customer delight, as even the most sophisticated digital technologies rise to the challenges that customers pose for them.

Here are the key steps to move to level 5:

1. Integrate historical monitoring data into machine learning and predictive analysis engines to allow for proactive preparation for anticipated failures.
2. Leverage automation to develop processes for self-healing infrastructures based on predicted failures.
3. Implement proactive service level monitoring allowing for redundant resource allocation, failover automation, and ultimately ‘lights out’ IT infrastructure management.

To support organizations looking to scale into level 5, LogicMonitor provides a rich API to give users the ability to programmatically query and manage their resources. This API enables users to develop processes that integrate with their own applications and triggers based on alerts to perform automated tasks to resolve issues.

With LM Service Insight, this new feature allows the grouping of monitored resources supporting a common service or application, aggregating the monitored data. Users can now not only keep data for ephemeral environments (Kubernetes, Docker, etc.) but also SLA tracking for a complete service or application -- not just the resource.

Level 5: Predictive

As with all maturity models, welcome to the wish list – the vision for how IT should behave in a truly digital organization.

In the case of IT monitoring, this endgame consists of self-healing infrastructure. Not only can organizations automate the discovery of root causes of issues and the mitigation of those problems, but they can also predict issues before they occur and take initiative to prevent them from happening in the first place.

Once the organization realizes this technology vision – admittedly at some point in the future – the enterprise will have achieved true 'lights out' operations. The entire technology landscape will be fully automated, and operations roles will shift to interpreting business needs. Such business intent becomes the only configuration the ops environment requires.

On the business side, leaders can rely upon their IT environments to rise to whatever challenge their customers throw at them. Not only is change constant and expected, but it also becomes a core competency of the organization. At that point, the full vision of digital transformation as customer-driven and technology-empowered becomes a reality.

THE INTELLYX TAKE: ALIGNING WITH THE MATURITY MODEL

Level 5 sets out a long-term vision for our IT organizations and our enterprises generally, but as with many goals, the value is in the journey.

Most if not all organizations are somewhere on this road. Today's state of the art is somewhere between levels 3 and 4, but even so, many organizations still struggle with the issues of levels 1 and 2.

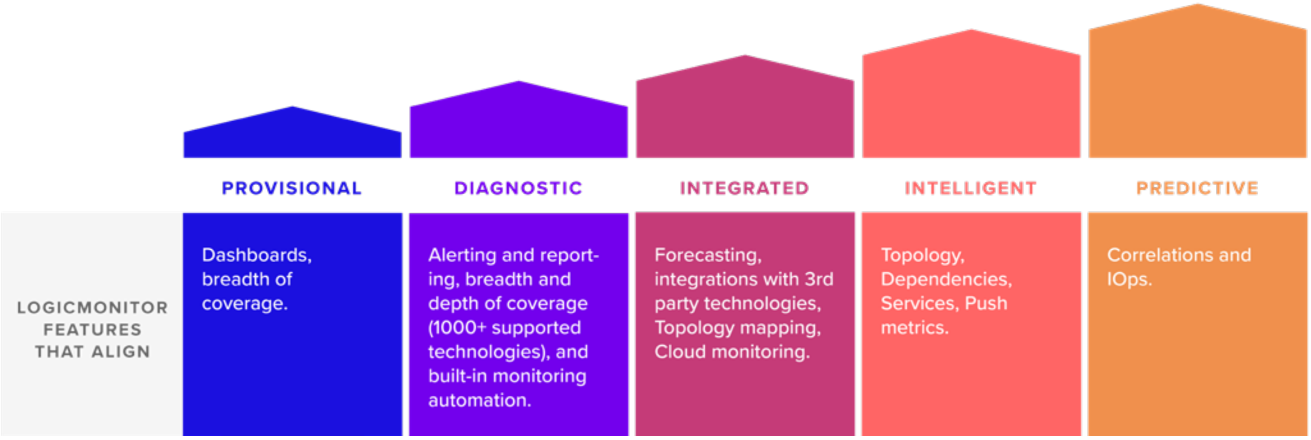
Regardless of the level of maturity of any particular organization, it's clear that every company should be looking to move past level 2. Simply adding one more tool to the mix – in other words, staying on level 2 – is not going to advance the organization toward its goals.

Instead, it's essential to select a monitoring tool that firmly places the ops environment at level 3, with a clear plan for level 4.

LogicMonitor is such a tool. True, it can help organizations at all levels 1 and 2, but its real value is levels 3 and above because of its strong hybrid monitoring capabilities.

For level 3 organizations, LogicMonitor provides forecasting, integrations, topology mapping, and cloud monitoring – essential to organizations who are moving to a cloud first infrastructure strategy.

As organizations move beyond level 3, then, LogicMonitor lays out a path to AIOps – AI-driven operational environments that can leverage LogicMonitor's intelligent approach to dependencies and business services.



	PROVISIONAL	DIAGNOSTIC	INTEGRATED	INTELLIGENT	PREDICTIVE
LOGICMONITOR FEATURES THAT ALIGN	Dashboards, breadth of coverage.	Alerting and reporting, breadth and depth of coverage (1000+ supported technologies), and built-in monitoring automation.	Forecasting, integrations with 3rd party technologies, Topology mapping, Cloud monitoring.	Topology, Dependencies, Services, Push metrics.	Correlations and IOps.

Regardless of the choice of monitoring tool, however, this IT monitoring maturity model can help organizations understand where they are on their path toward digitally transforming their operational environment, and what steps are needed to achieve their short-term and long-term goals for their infrastructure as well as their business at large.

LogicMonitor and ServiceNow are Intellyx clients. At the time of writing, none of the other organizations mentioned in this article are Intellyx clients. Intellyx retains full editorial control over the content of this paper.