Negotiating Cloud Application Change and Risk with Observability

An Intellyx Analyst Guide for Evolven

By Jason Bloomberg and Jason English

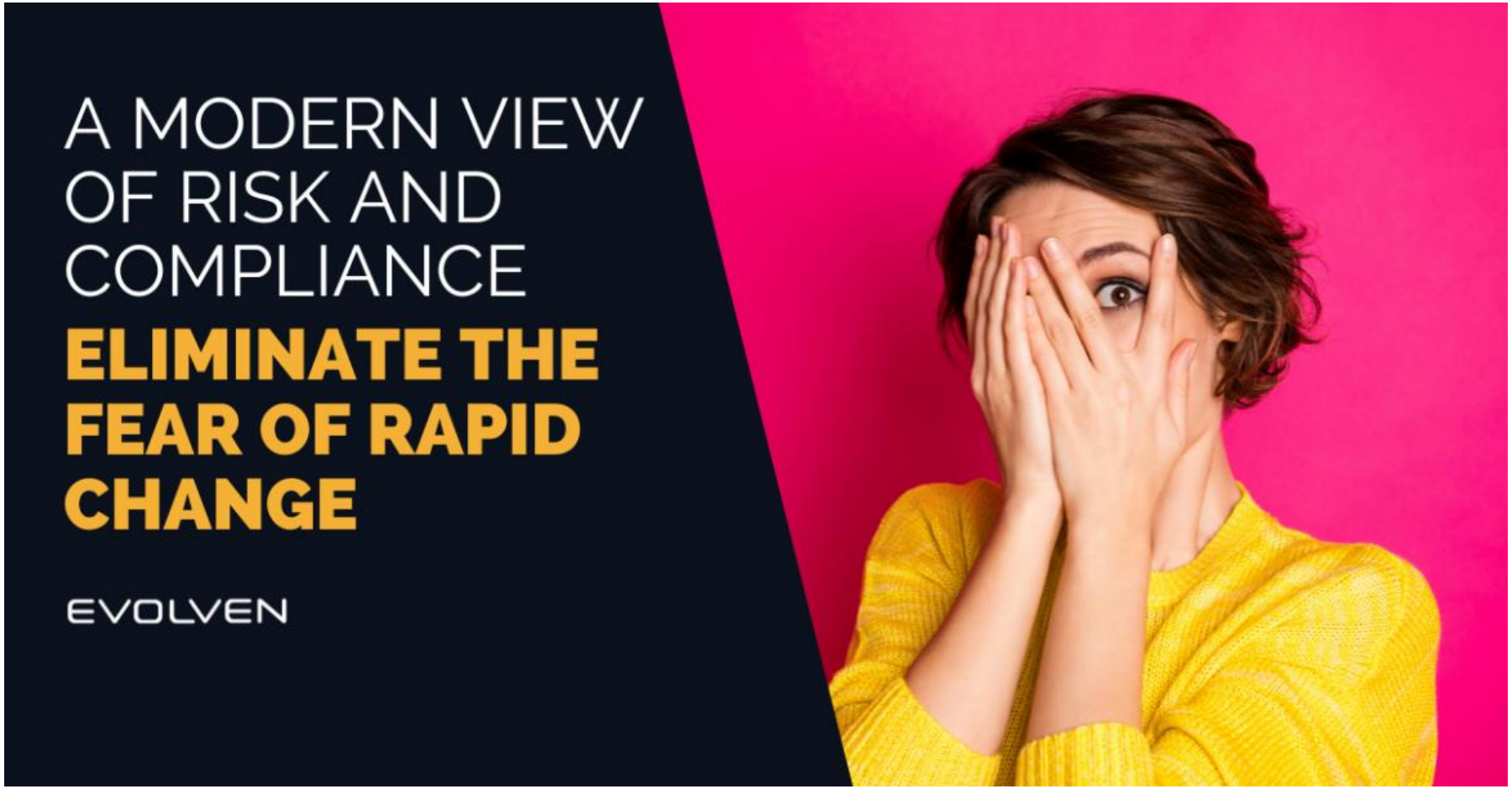
Table of Contents

Introduction

Since the advent of cloud computing, containers and Kubernetes, much has changed, and not just within the configuration and patches going on behind the scenes of our broad Hybrid IT application and data estates.

A massive movement toward remote and hybrid work patterns, accompanied by an explosion of distributed cloud services atop legacy systems and the use of continuous delivery automation has made it all but impossible for IT Ops teams and SREs to keep up with the rate of change and configuration drift when assuring application stability.

To get ahead of new risks like ransomware and software supply chain disruption, we now need change control and risk management across an enterprise IT environment in conjunction with ITSM and observability platforms. This Intellyx guide, sponsored by Evolven, will help readers negotiate that risk, by finding new insights at the heart of DevSecOps practices.



By Eric Newcomer

CTO and Principal Analyst, Intellyx

They say the only constant is change, but for IT the pace of change is not just constant: it's constantly accelerating.

This puts a ton of pressure on IT dev, sec, and ops teams because change is the primary cause of failure.

Business goals frequently conflict with security and risk mitigation controls, and it's hard to maintain the balance between rapidly improving an app's user experience and keeping systems compliant, available, and safe. The result is often security and compliance gaps, despite the best of intentions.

Compliance systems struggle to keep pace as more and more business and government services go online, and as more and more sensitive data is put at risk.

The need for security policy and procedures earlier in the development process – known as shift left – is no longer a desire but a must as enterprises balance agility with quality delivery and the ultimate user experience.

In the end, constant change and increasing complexity drive the need for updated security, risk, and compliance processes that can keep up, and not impede the inevitable march toward digital progress. Evolven's framework meets this need.

The challenge of usability

Unlike internally focused IT systems for employees, it's impossible to predict in advance how an external customer will respond to a user interface.

Best-in-class digital apps, such as you find in retail, push changes to production multiple times a day and rely on continuously collecting and analyzing user interactions and feedback to fix and improve the apps.

However, gathering feedback based on personal data for usability improvements can cross the line into privacy violations and can trigger a compliance review or legal action.

This use of personal data results in increased regulation, risk mitigation, and compliance with a range of legal and social requirements to protect such personal data and individual privacy, while keeping systems running 24x7.

The Evolven solution provides organizations with essential visibility into the ever-changing configuration state of its IT environment, showcasing risks, enabling necessary safeguards, and eliminating the fear of rapid change by providing the needed safety rails.

Modern compliance requirements are also changing rapidly

An increase in the number and scope of certification standards and regulations governing security controls and system configurations has been a natural result of the increasing digital presence in our lives.

Continuously emerging regulations and compliance frameworks such as CIS, PCI, NIST, OCC, and others, specifically identify change and configuration management requirements that IT teams must decide how to implement.

IT risk and compliance managers must therefore continuously monitor the impact of configuration change due to various external regulatory compliance mandates.

A good example is the recently-issued SEC mandate called "T+1" which requires financial institutions to settle trades within one day instead of the current two days – all by May 2024. This will greatly impact IT systems, including configuration, in order to achieve compliance.

Evolven provides a "single pane of glass" interface for IT, risk, and compliance management staff to assess the impact of such change and support the work of auditors.

Preventing outages and incidents

Governance is necessary, especially when delivering code changes more and more frequently. Ungoverned change is a frequent cause of incidents, breaches, and outages.

Organizations face the challenge of resolving the internal tension between an organization's dev and ops teams. Dev wants rapid release; however, ops wants to avoid risk.

Anticipating the impact of a configuration or code change at any time means capturing pertinent data continuously, using AI to predict risk, and doing this as close to real-time as possible. Consolidating the data into a holistic view across in-scope infrastructure and applications is the only way to present a meaningful view.

The holistic view requires collecting data from monitoring systems, configuration databases, code management systems, automated testing systems, and so on. Major stakeholders – IT Ops, production support, security, and dev management can all have their own views into the impact of change analysis.

This allows you to analyze and prioritize the impact of changes to configuration, data, and capacity across the organization, and not simply look at the impact of code changes. Application code does not run in isolation.

Modern AI analytics engines take the firehose of data relevant to configuration and change control and do this for you. Evolven can predict the impact or risk of a proposed change before you roll to production.

AI analysis such as this raises warning flags and provides guidance based on past history.

By utilizing its CI/CD Risk Gateway, Evolven's solution automates traditional CAB functionality and prevents incidents and outages before they happen.

After the fact analysis

While it's best to prevent incidents and security breaches before they occur, it's equally important to rapidly respond to them after the fact. It's critical to rapidly correct the problem, but also to establish the root cause and put measures in place to prevent a recurrence.

The same system that collected all the data to predict (and prevent) the risk of a change can help identify the root cause of an incident or breach and recommend changes to repair the issue.

Auditors and regulators want access to all the relevant data about all the components of the system, as well as the log of the decisions made based on the risk analysis, whenever there's a significant breach or incident.

The Evolven Configuration Risk Intelligence Solution not only detects configuration changes to predict incidents and outages before they occur, it also analyzes them after the fact to identify the root cause quickly and help prevent future occurrences.

The Intellyx Take

The rapid pace of digitization globally across businesses and government, and the associated risk of outages and breaches have caused an increased focus and need for compliance and regulation.

Rather than slowing down the pace of progress, however, risk and compliance systems need to keep pace. Advanced AI offers compelling capabilities for predictive analysis that can catch problems before they occur. The same systems can help remediate and prevent incidents from occurring again.

by Jason Bloomberg

Managing Partner and Analyst, Intellyx

Along with making and saving money, managing risk is one of the top three priorities for any executive.

As with financial motivations, dealing with risk must percolate through the entire organization. Everyone is responsible for managing the risks within their respective purviews.

IT executives in particular must manage risks in their organizations. Downtime, performance issues, and compliance gaps all threaten the health of the business and thus are risks that the entire IT organization must manage.

Managers must make investment decisions that manage and mitigate all such threats across the board, without irrationally emphasizing one type of threat over another.

They need some kind of common denominator that gives them such balanced, rational control over risk. A new generation of configuration management can provide that common denominator.

How to Quantify Different Types of Risk

Of all the risks facing the enterprise at large, many fall within the domain of IT. We'll consider three types of risk:

- *Availability risk* – the risk of downtime, as well as the risk of poor performance that adversely impacts user experience. Such risks threaten the organization's bottom line via lost business and customer churn.
- *Compliance risk* – the risk of fines and reputational damage due to regulatory non-compliance.
- *Cybersecurity risk* – the risk that vulnerabilities will lead to breaches, causing loss of data and money, as well as reputational damage.

Other risks face the IT organization like technical debt risk, but the three categories of risk above are the most prominent.

Without a common understanding of these risks, managers are likely to make irrational investment decisions based on the crisis of the day. Organizations must objectively quantify the risks they face. This quantification relies on the practice of *risk scoring*.

Risk scoring begins with risk profiling, which determines the importance of a system to the mission of the organization. Risk scoring provides a basis for quantitative risk-based analysis that gives stakeholders a relative understanding of the different types of risks.

The overall risk score is the sum of all the risk profiles across the type of risk in question and thus gives stakeholders a way of comparing risks in an objective, quantifiable manner.

One particularly useful (and free to use) resource for calculating risk profiles and scores is Cyber Risk Scoring (CRS) from NIST, an agency of the US Department of Commerce. CRS focuses on cybersecurity risk, but the folks at NIST have intentionally structured it to apply to other forms of risk, including availability and compliance risk.

If an organization has a quantitative approach to risk profiling and scoring, then it's possible to benchmark risks to compare one type of risk to another – and furthermore, make decisions about mitigating risks across the board, and how much money to spend doing so.

Risk scoring is one aspect of the broader challenge of *risk assessment*. Organizations must assess their risks to coordinate various risk mitigation efforts that lead to an optimal balance between risk mitigation and the costs of achieving it.

There are, in fact, several different risk assessment frameworks that organizations can use to quantify and manage their IT risks, including the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework, the NIST Risk Management Framework, COBIT 5 for Risk, and ISO/IEC 27005:2022.

These frameworks and standards can help organizations assess and quantify their risks across different types of risk. Once they have quantified their various types of risks, they are now able to make informed decisions about how to mitigate all risks within the context of the budget for managing IT risk overall.

Closing the Gaps Between Risk Assessment and Mitigation

Once the organization has a handle on the IT risks it is facing, it's well-positioned to mitigate those risks. However, no risk scoring and assessment regime, no matter how complete, can identify all the risks that threaten the organization.

There are many types of threats that can fall through the cracks, including zero-day attacks, mistakes due to human error, and new vulnerabilities that result from a change in configuration.

For all these reasons, organizations must leverage technology that goes beyond assessment checklists, capturing the vagaries of real-world situations that go beyond assessments and their associated benchmarks.

To close these gaps organizations must manage the configurations of the various systems, applications, and networks that make up the IT estate.

Misconfigurations can lead to performance issues and downtime. They can also lead to out-of-compliance situations. And most significantly, misconfigurations can be the root cause of vulnerabilities that lead to breaches.

Misconfigurations, therefore, are often at the heart of availability, compliance, and cybersecurity risk. Finding the root cause misconfiguration that presents a particular threat requires some detective work using a configuration risk intelligence tool like Evolven.

Regardless of the type of risk, operators can use Evolven to trace interaction paths from applications to databases, uncovering the root cause misconfiguration along the way.

Evolven monitors the entire configuration estate enterprise-wide in real-time for any change, anomaly, or misconfiguration, looking beyond the frameworks and checklists to prevent, as well as mitigate, issues.

The risk-based AI engine analyzes changes as they occur and prioritizes them based on risk, enabling a more proactive posture to risk management across the enterprise.

The Intellyx Take

Leveraging a risk assessment framework to quantify risk is a daunting task. It can lead to massive reams of paperwork, suitable perhaps for auditors but ill-suited to managing the risks themselves.

It is important, therefore, for organizations to think beyond the scorecards, assessments, and benchmarks by implementing proactive configuration management.

Quantifying and measuring risk is important for making informed decisions about managing the threats to the organization, but don't let the measurement process prevent your team from focusing on the actual management of risk itself.

By Jason English

Partner and Principal Analyst, Intellyx

Most of us have never had to think about enterprise digital risk, in all its forms.

Until recently, only a select council of IT executives needed observability into a broad range of potential software and hardware problems. They would all get together for a quarterly or monthly risk management review board meeting, either in person or on a very long, monotonous conference bridge.

The 'telemetry' on this call would consist of a CIO or a Chief Risk Officer, asking each department head, from cybersecurity to development, to IT operations, regional managers, and application suite owners: "What issues are getting reported to you? What are you seeing in your dashboard?"

In some ways, this occasional drudgery was pretty effective at mitigating risk because early change management and compliance procedures were slowing things down to a manageable pace. Then, we started introducing increasing levels of agile software updates and delivery automation atop cloud infrastructures.

Change happens so fast in today's hybrid cloud environments, it's much harder for enterprises to truly identify and control the risks that matter from the myriad of potential IT risks. Further, with so many stakeholders making changes that could impact upstream or downstream services, risk mitigation is quickly becoming part of everyone's job.

Clarifying the opaque silo problem

Talk to a big 4 consultant about risk, and they will likely say that your enterprise "needs to break down informational silos to gain visibility into shared risk mitigation objectives." Or some sort of win-win management-speak like that.

While cracking open silos always sounds nice in theory, what if they are still holding valuable products inside? It is important to remember that information silos were established for a reason. Different metrics matter to Ops, Dev, and Security teams because they have different objectives.

IT Ops teams will use their ITOM and ITSM platforms to track infrastructure performance indicators and resolve issues, whereas DevOps teams are carefully monitoring their CI/CD pipelines and deployments to manage faster, higher-quality releases. Security teams scan for threats and vulnerabilities in their SIEM and XDR workflows. Partners may have their own ways of measuring their service's API performance against SLAs and SLOs in relation to your enterprise.

Even if you could gain an "X-Ray Vision" superpower and give everyone transparency into each other's silos, each of these teams would likely not understand the context of the data they are looking at for their own workflows.

The modern SRE (site reliability engineer) role would be the closest to understanding the meaning of risk indicators within each group's siloed dashboard, but even then, total transparency would only overwhelm them with unfiltered data when they are trying to identify risks.

Visibility requirements across different dimensions

Teams will never have total transparency into each other's operational dimensions, but they will always collectively need to share visibility into what really matters: preventing and mitigating system-wide risks that will impact customers.

There's no simple way to avoid risk in today's fast-changing enterprise architectures, but there are requirements for improving visibility.

Observing complexity at scale. Any well-established enterprise that intends to survive has already embarked on modernization initiatives to improve its scalability and support new business services while maintaining operational integrity.

This leaves them supporting a mix of existing on-prem core systems and data stores, third-party service integrations, cloud data warehouses and thousands of server instances, Kubernetes clusters and serverless functions running in different clouds.

The new digital landscape is changing every few seconds. When something bad happens, finding the root cause is a lost cause. What is the key information needed for tracking down the problem, and going back to the time when it worked?

Hybrid IT telemetry. The information needed to identify hybrid IT application risk doesn't reside within one silo. There are readily available platforms for service management, and cloud tools for monitoring and optimizing AWS instances that don't talk to Azure or GCP instances.

The open source and vendor community are building excellent tools for Kubernetes observability, telemetry, and container orchestration, but by nature, those tools focus on specific clusters and workloads that run wherever they make the most sense across distributed infrastructures.

Predictive change intelligence. The DevOps movement brought agile software delivery and CI/CD automation to the forefront, and with it, codified approaches to configuring, testing, staging, and delivering new application code and IaC (infrastructure as code) components.

Despite all of this shift-left test automation and deployment goodness, how can we know what will happen when these changes actually move into production, and interact with the rest of a distributed application estate?

Establishing enterprise-wide visibility

Since heterogeneity will never go away in a hybrid IT environment, we need to gain enterprise-wide visibility into information that doesn't just reside in one silo.

Cloud management, service management, release management, and analytics vendors often describe their highest-level global view as a "single pane of glass" (or, SPOG), providing a universal view into the many operations performed—within their own management dimensions.
In reality, there are many single panes of glass out there. How can we make sense of them?

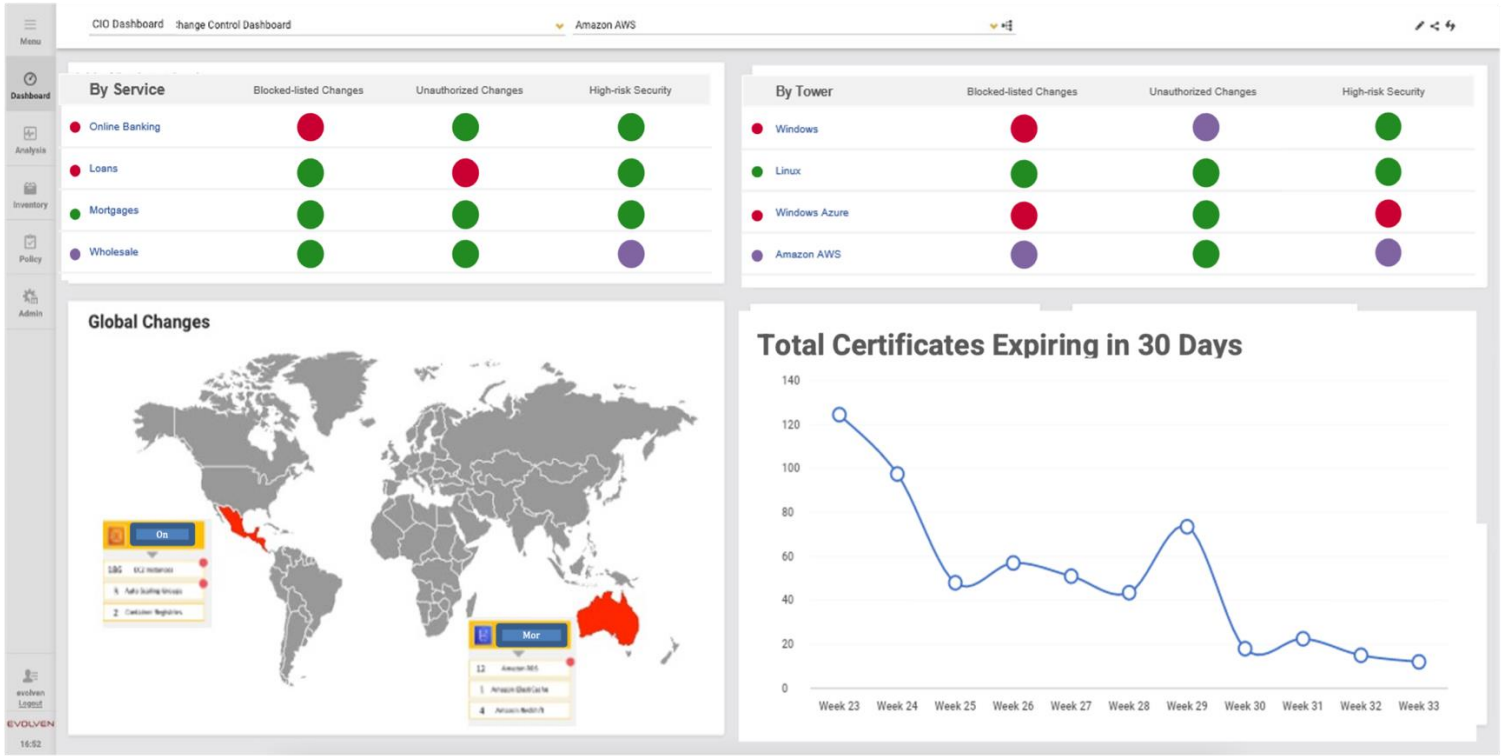


Figure 1: Enterprise-wide multi-system risk management dashboard in Evolven.

Rather than dictating a particular IT asset or service management suite, **Evolven** has taken a non-opinionated approach to identifying enterprise-wide configuration risk, with agentless collection of near-real-time data from a distributed inventory of cloud and on-premises systems and services, and the platforms that deliver, monitor, and secure them.

Yes, it's another SPOG, but think of it as a single view of the data that would be relevant to the modern version of that enterprise-wide risk control board, which now has more participants and stakeholders than ever.

Operationalizing risk management at a fintech

A major financial technology firm used Evolven to roll up a unified view across more than 250 thousand enterprise-wide systems, services, configuration, and usage data sources at hourly or up-to-the-minute intervals, depending on the rate of change.

What was really interesting is how they operationalized the use of the single view, automating some alerts with rules-based policies, while empowering IT leaders to ask triage questions of the systems within their own domains for every flagged change, such as:

- *Is this change verifiably authorized or not?*
- *Is the change consistent with other similar changes?*
- *Is there anything anomalous about the change we are looking at?*
- *Does the change impact our standing for compliance or contractual agreements?*

In this scenario, Evolven provided visibility into system-wide risk and helped the team surface the changes that presented the most risk. But success requires more than a single pane of glass. The firm's disciplined team operationalized their risk review practices and escalation process to extract the most value from that visibility.

The firm created their own cloud data lake to accept event logs for things like change requests, expired certificates, and configuration drift, purpose-built for running their own risk modeling and projections. Alerts and incidents coming out of this process were then routed with a contextual data report to the appropriate database team or service management system.

A welcome side effect—or perhaps the best value for the teams responsible for compliance—was how well the system-wide snapshots and change reports documented the company's system availability, data protection, and security postures. Auditors told them they were light years ahead of the competition as they passed compliance exercises with flying colors with little or no additional effort.

The Intellyx Take

Just giving teams a better reporting or monitoring tool for managing risk is never going to solve the risk visibility problem by itself.

Like any other digital transformation, achieving enterprise-wide risk awareness requires people, processes, and technology—in that order.

The best performing organizations always build up their own agreed upon taxonomy and procedures for getting data out of key systems, distributing it to the right people to manage risk, documenting or codifying the results for continuous improvement, and connecting that output to the systems of record each group uses.

About the Analysts

Jason Bloomberg is founder and managing partner of enterprise IT industry analysis firm Intellyx. He is a leading IT industry analyst, author, keynote speaker, and globally recognized expert on multiple disruptive trends in enterprise technology and digital transformation.

Mr. Bloomberg is the author or coauthor of five books, including *Low-Code for Dummies*, published in October 2019.

Jason "JE" English is Partner & Principal Analyst at Intellyx. Drawing on expertise in designing, marketing and selling enterprise software and services, he is focused on covering how agile collaboration between customers, partners and employees accelerates innovation.

A writer and community builder with more than 25 years of experience in software dev/test, cloud and supply chain companies, JE led marketing efforts for the development, testing and virtualization software company ITKO from its bootstrap startup days, through a successful acquisition by CA in 2011. Follow him on Twitter at @bluefug.

Eric Newcomer is CTO and Principal Analyst at Intellyx, a technology analysis firm focused on enterprise digital transformation. Eric is a well-known technology writer and industry thought leader, and previously held CTO roles at WSO2 and IONA Technologies.

About Intellyx

Intellyx is the first and only industry analysis, advisory, and training firm focused on customer-driven, technology-empowered digital transformation for the enterprise. Covering every angle of enterprise IT from mainframes to cloud, process automation to artificial intelligence, our broad focus across technologies allows business executives and IT professionals to connect the dots on disruptive trends. Read and learn more at https://intellyx.com or follow them on Twitter at @intellyx.

About Evolven

As the pioneer of AIOps and Configuration Risk Intelligence, Evolven automates configuration and change controls across the hybrid cloud. Using AI-based analytics, Evolven detects and prioritizes risks triggered by actual, granular changes in configuration, application, infrastructure, and data, to help prevent and rapidly resolve stability, compliance, and security issues. With Evolven, DevSecOps, CloudOps, and ITOps teams experience greater visibility into your environments resulting in greater productivity, fewer incidents, and faster MTTR.

For more information, go to evolven.com.