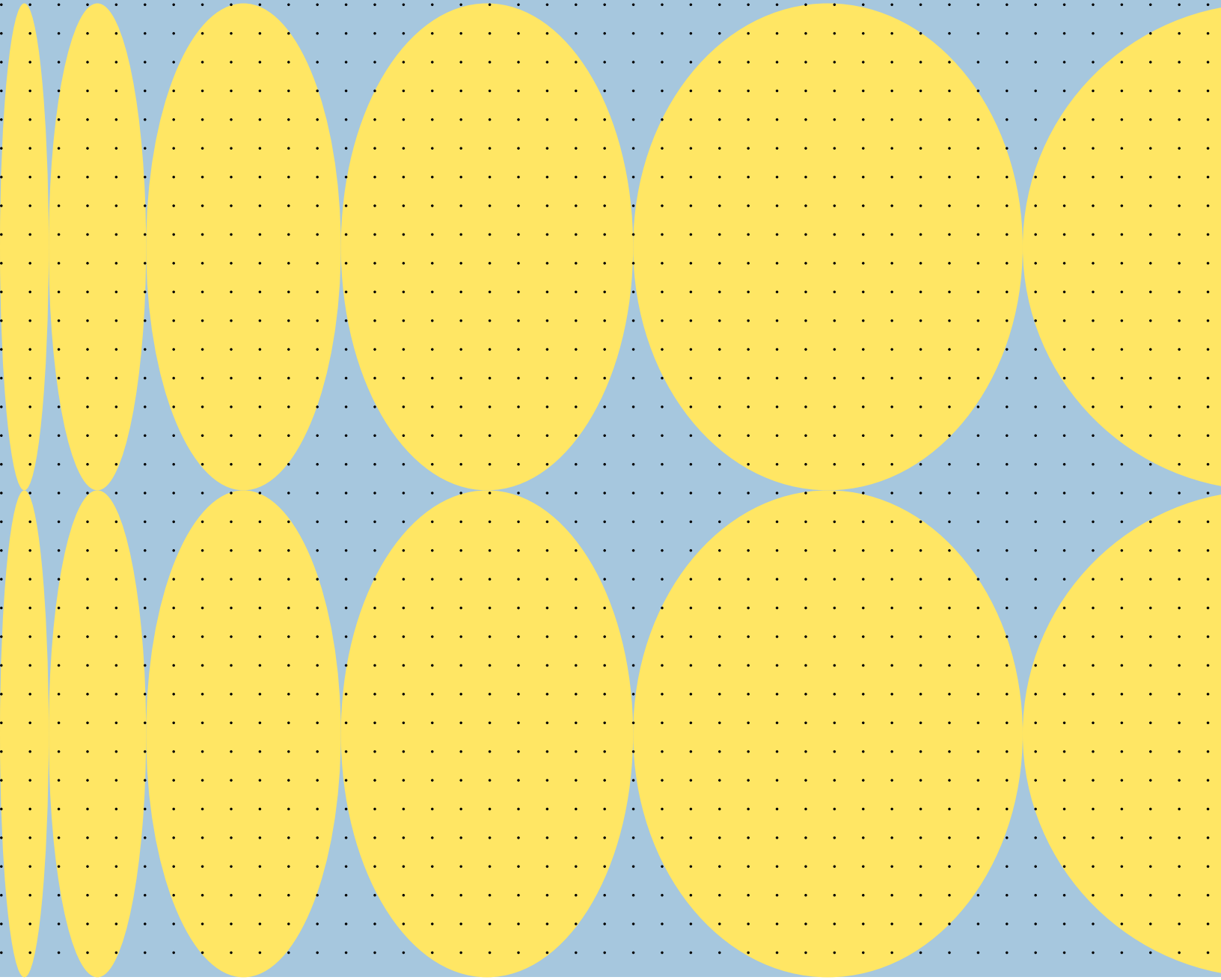

Accelerate Transformation with Digital Operations Management for Financial Services

Laying the Groundwork to Win in Digital

PagerDuty

Table of Contents

Under Pressure: Winning in Digital Is a Business Imperative

Financial services institutions have been facing pressure to modernize for years, but legacy architecture and processes, along with compliance regulations have made it difficult for teams to innovate faster.

New competitors that offer a digital-first model and other recent trends have further accelerated the need for financial services to reflect on how to deliver on a better digital customer experience.

In an increasingly consumer-centric world, traditional financial services institutions need to adapt and embrace some of these new models to keep up and compete.

Why Digital Operations Management Matters for Financial Services

Effective, digital operations management is urgent and mission-critical, no matter which business you are in. In financial services, however, it's especially crucial. The highly competitive nature of the industry, threat of disruption from fintech startups, heavy reliance on legacy infrastructure, and unique compliance and security requirements pose additional challenges for financial services institutions.

Here are some areas of investment and modernization that financial services can (and should) embrace:

- **Platforms and Technology.** Adopting best-of-breed, decentralized cloud platforms, and technology with API-first design methodologies that can easily integrate with technical teams' platform of choice allows institutions to more easily access automation, extensibility, flexibility, and auditability.
- **Talent.** Empower talent to "work where they want" while also ensuring a single-pane-of-glass view of relevant information. Additionally, democratizing uniform operational practices like on-call rotations, escalations, and incident triage can dramatically reduce responder burnout and fatigue. It also leads to better engineering productivity and higher talent retention.
- **Culture.** The philosophy of real-time communication and collaboration that the DevOps model encourages can help foster a leaner system where bottlenecks are solved in a manner that not only fixes the problem, but also improves the process.
- **Process.** Significantly improve processes for alerts and incidents through iterative efficiencies like dynamically executing runbooks, in addition to implementing incident bridge automation, proactive and relevant stakeholder updates, and blameless postmortems. Apart from optimizing team and service performance, process improvements can lead to rigor and accuracy in adherence to compliance and regulatory requirements.

Challenges in Financial Services

Understanding why the stakes of digital transformation are so high for financial services companies begins with identifying their unique challenges.

INDUSTRY REGULATIONS: COMPLIANCE & SECURITY

Financial services is one of the most, if not the most, highly regulated industries in the world, which makes it particularly challenging to meet heightened expectations for service quality.

For example, when responding to a service disruption, teams need to know which systems are subject to regulatory compliance controls or host regulated data because they may need to explain to auditors how a problem was resolved. They may also need to prove that all resolution steps were in compliance with guidelines in order to avoid potential fines and damage to the brand. This creates an extra layer of complexity that needs to be managed when responding to an incident.

Maintaining security is also crucial because security problems are especially damaging in the financial services industry. Beyond the compliance considerations related to security, companies can face serious consequences for failing to protect the security of systems and customer data. For example, security negligence that leads to hacked bank accounts can deal a tremendous blow to customer loyalty. It can also lead to lawsuits and, of course, significant monetary loss due to theft.

HIGH CUSTOMER EXPECTATIONS

Today's digitally savvy consumers have grown to expect convenient and innovative services at all times. Providing basic banking is no longer enough, and service breaks like maintenance windows can sour the customer experience. Customers are demanding value-adds such as budget planning help available across channels, mobile banking functionality, and 24×7 service availability. Meeting these expectations is difficult for companies whose infrastructure was not originally designed to handle them.

Financial services institutions are also constantly challenged to keep up with digital-native startups that have been built in the cloud and are designed to deliver on these exact customer demands. Today's fintech startups are able to quickly bring consumer-ready innovations to market because they leverage agile business models (like internet-only banking and mobile payments) and innovative financial products (such as blockchain-based cryptocurrencies) that help companies lower transaction costs and provide new security and privacy benefits.

LEGACY INFRASTRUCTURE & GROWING COMPLEXITY

In most cases, financial services institutions that have been in business for decades still depend on infrastructure that is decades-old. To make matters more complicated, this infrastructure is usually intermixed with newer systems.

Even if some workloads have been moved to the cloud or other more modern environments, many traditional companies in this market continue to run mission-critical operations on mainframes. You may offer customers a mobile banking app that is compatible with the latest iPhone, but there is a good chance that the foundation of the technology stack that drives that app considerably predates the introduction of the smartphone.

Adding to the infrastructure complexity of financial services institutions is the need (in some cases) to keep both physical and virtual infrastructure running smoothly. If you're a bank, customers expect to be able to access your services at a local branch, an ATM, or online. Ensuring that all services remain up and running requires the complex array of hardware and software on which they depend, as well as management of support personnel for both software and hardware systems. These requirements make infrastructure management in financial services especially difficult; unlike in most other industries, 24×7×365 support needs are not limited to the IT realm alone.

Balancing Digital Innovation With Industry Regulations

In order to handle these challenges and thrive in an increasingly dynamic, highly competitive environment, traditional financial institutions should continue to embrace digital transformation and innovation while balancing regulatory needs.

Keeping up with the pace of innovation required to acquire and retain digitally savvy customers means financial services institutions need to invest in their people, technology, and processes to empower your technical teams to stay agile and productive.

However, a key side effect of creating and delivering innovative digital customer experiences is increased complexity, and as systems and teams get more complex, it becomes impossible to efficiently manage everything in a purely centralized fashion. This can be especially painful when it comes to incident response because when incidents happen, siloed systems and teams operating in traditional models can create a domino effect that can negatively impact the customer experience and put your business at risk.

Using Digital Operations Management to Accelerate Digital Transformation

Service failure and the real-time work associated with getting it back online is an inevitable part of operating with technology and systems. But how your company responds when that happens makes all the difference when it comes to the customer experience and, ultimately, your revenue.

Spending the time to evaluate what technology signals to monitor, identify which people to engage for what context, and define how processes tie them all together in a coordinated approach are all parts of digital operations management.

The main goal of having a digital operations management platform in place is to intelligently orchestrate a coordinated response to incidents that reduces resolution time and limits the damage and impact to the end customer.

For financial services, digital operations involves several components:

End-to-End Visibility
It is important for any digital business to maintain a holistic view into the health of its IT infrastructure. Different monitoring tools can provide full-stack visibility, allowing teams to keep an eye on IT infrastructure health.

In financial services, digital operations management tools need to support not just modern infrastructure, such as applications hosted in the public cloud, but also legacy systems like mainframes. To quickly triage and effectively troubleshoot problems, teams require a clear line of sight across environments, applications, and services so they can map service dependencies, distinguish noise from meaningful information within their monitoring data, and recognize when multiple alerts stem from a common problem.

Built-in Automation and Context

Optimizing digital operations with a focus on urgent, real-time work makes it possible for you to find out about critical, customer-impacting incidents before your customers do. By adding automation to your incident management workflow, your team can benefit from proactive detection of issues, automated grouping of related monitoring alerts (as well as suppression of non-actionable events), and dynamic routing of issues to the right people based on the service impact. Automation also allows you to standardize and make repeatable those processes that would otherwise be error-prone and done manually.

Automated notifications should be delivered in real time, and contain all the critical machine and personnel information required to eliminate context switching and enable rapid remediation.

Business-Wide Orchestration for Real-Time Work

Once it's determined that a signal is urgent, actionable, and impactful, it must be routed to be fixed as quickly as possible. There are three key components of managing operations in real time:

- **Incident response** is a process that helps teams route actionable signals to the right people, at the right time, with full context so they can be empowered to orchestrate a swift response. To learn more about modern incident response best practices, read **this ops guide**.
- **Full-service ownership** is an operational model where development and operation teams have complete ownership over every aspect of the services they support: from design and development, to production operation, and the eventual sunsetting of their software. To learn more about Full-Service Ownership, read **this ops guide**.
- **Collaboration and communication** are key to help coordinate incident management quickly between different parts of your organization. For example, software developers and hardware technicians may need to collaborate when responding to a broken ATM. Support personnel may need to notify customers quickly when a service is down. Your legal department might be required to assist in responses to issues with legal consequences. To learn more about communications practices for incident management, read **this ops guide for internal stakeholder communications** or **this ops guide for business incident response.**

A Final Note About Security

An effective digital operations management platform plays a key role in ensuring that a financial services institution can maintain its security posture, which is vital in this industry. First, it ensures that notifications about security alerts reach the right engineers in real time, while improving the signal-to-noise ratio. It also helps coordinate an orchestrated response across teams—which may include not just security engineers, but also your legal team, developers, system admins, and other personnel.

By delivering prompt security notifications and enabling effective response orchestration, the right incident management platform can help you address security breaches before compliance requirements and/or customer trust are compromised.

For more information on best-practice security incident response, see the security incident response documentation from PagerDuty **here**.

Sign up for a free trial

To learn more about PagerDuty for Financial Services,
visit **www.pagerduty.com/industries/financial-services/**

About PagerDuty

PagerDuty, Inc. is a leader in digital operations management. In an always-on world, organizations of all sizes trust PagerDuty to help them deliver a perfect digital experience to their customers, every time. Teams use PagerDuty to identify issues and opportunities in real time and bring together the right people to fix problems faster and prevent them in the future. Notable customers include GE, Cisco, Genentech, Electronic Arts, Cox Automotive, Netflix, Shopify, Zoom, DoorDash, Lululemon and more.

To learn more and try PagerDuty for free, visit www.pagerduty.com.

PagerDuty