# UNLOCKING THE POWER OF DATAOPS FOR SUCCESSFUL BUSINESS OUTCOMES

Today's organizations are committed to collecting and analyzing as much data as possible from sources new, old, and evolving. But they continue to have variable levels of success distilling and yielding value from it. The data itself isn't necessarily the problem. Instead, it's where that data is sourced and how it's used—plus the people, processes, and technology it encounters along the way—that can either amplify or obscure its value.

The explosive growth in data in recent years has spawned its own operational category: DataOps. And how well organizations incorporate DataOps best practices makes all the difference to successful data management and corresponding data-driven outcomes.

*Putting the "Ops" in DataOps: Success Factors for Operationalizing Data*, a recent report from BMC in partnership with 451 Research and S&P Global, found that defining a successful DataOps approach comes down to what you want your data to do for your business. And that approach needs to be tailored to your organization's specific conditions and objectives.

Factors contributing to data-driven business success are often as variable as the demographics of the organization. Business size, geography, data management maturity, DataOps best practices, the operating model for data management and data delivery functions (whether centralized, federated, or hybrid), and the application of technologies such as artificial intelligence and machine learning (AI/ML) in data management can all influence how much business value an organization creates from its data.

DataOps is the key that will enable businesses to unlock the door to greater agility and resilience

amid a fluctuating economy and increasing competition and regulatory requirements. But this means successfully implementing DataOps practices, technologies, and expertise to get the most out of their data management initiatives.

In our report, we rank an organization's maturity based on its data management strategy, practices, and architecture. The four data management maturity profiles are:

- **Developing:** Strategy is developing, but practices and architecture may not yet be closely linked to critical business outcomes.
- **Functional:** Strategy is largely developed, with some high-priority data practices and architecture linked to critical business outcomes.
- **Proficient:** Strategy is fully established, with nearly all data practices and architecture linked to critical business outcomes.
- **Exceptional:** Strategy is perpetually optimized, with data practices and architecture driving novel sources of value.

## Data governance considerations

Of particular interest to European companies is the ever-growing list of compliance requirements, especially in customer data protection and personally identifiable information (PII). A significant number (65 percent) of survey respondents said they are currently collecting and/or actively managing data specifically to support their corporate governance or responsibility initiatives.

According to the report, " the data-driven regulatory landscape continues to proliferate and become more nuanced across geographies and sectors, organizations with developing maturity will likely need to allocate resources toward meeting 'reactive' external requirements just as much as they allocate resources for more 'proactive' efforts toward business value generation with data."

As we've seen with recent worldwide data leaks and hacks, mishandling customer data can have far-reaching consequences for a business, from significant fines and scrutiny to reputational harm that damages relationships with customers, partners, and suppliers. Externally imposed mandates and regulatory requirements can be a useful call to action for organizations to exert more granular control over their enterprise data resources, with added benefits that go beyond simply meeting the regulatory considerations.

The report finds that exceptionally mature organizations have already systematically addressed externally imposed, defined, or prescriptive requirements related to data management and control. That said, those organizations still need to be both forward-looking and collaborative, keeping pace with the reality of their technological capabilities. By doing so, they can prepare for future requirements and collaborate with regulatory bodies or partner organizations to define what is appropriate and defensible in terms of data stewardship and control.

## DataOps and regulations

Another key finding in the report is that European organizations are leading the way in active data management practices that leverage emergent technologies. They also tend to be more highly regulated in terms of data-related compliance and AI requirements. Case in point: the Digital Operational Resilience Act (DORA) is set to take effect across the EU on January 17, 2025.

The act is designed to enhance the operational resilience of digital systems that support financial

institutions operating in European markets. It's intended to guide organizations in building resilient frameworks, with a comprehensive focus on service visibility, risk mitigation, business continuity, incident management, and governance. Under this new legislation, shared information must comply with relevant guidelines, and PII must meet the criteria of the EU's General Data Protection Regulation (GDPR). By establishing sound DataOps practices, EU organizations can be ahead of the competition in compliance readiness.

## Data compliance considerations

The Digital Operational Resilience Act covers five considerations that organizations should keep in mind as they move toward compliance, all of which apply to data:

- **Identification:** Understanding risk to systems, people, assets, data, and capabilities, including business context, policies, and vulnerabilities.
- **Protection:** Ensuring safeguards to limit or contain the impact of a potential cybersecurity event. Fortifying defenses to ensure the integrity and security of critical data and systems.
- **Detection:** Discovering threats, cybersecurity events, and anomalies in real time and understanding their potential impact for swift mitigation.
- **Response:** Taking action to limit the impact of those threats, cybersecurity events, and anomalies with well-defined response mechanisms and protocols in place.
- **Recovery:** Ensuring systems can return to normal conditions efficiently and effectively.

Data is an important business driver—for some, the primary business driver—so getting a handle on it, as well as the people, processes, and technology that maximize its value, is an organizational imperative.

You can read the entire report here, and take the data maturity assessment here to find out where your organization is in its development and which areas you need to address to leverage data for successful outcomes.