Predicts 2021: Value Streams Will Define the Future of DevOps

Published 5 October 2020 - ID G00734377 - 23 min read

By Daniel Betts, Chris Saunderson, **and 4 more**

To accelerate development and enable continuous delivery of customer value, organizations need to reach the next level in their agile and DevOps practices. I&O leaders and application leaders must focus on value stream management to maximize flow, improve delivery efficiency and drive innovation.

Overview

Key Findings

- To deliver customer value faster, organizations need enhanced visibility, orchestration, integration and governance management across DevOps value streams.
- Traditional auditing, security and compliance checks are often performed manually, which restricts delivery flow and introduces unacceptable levels of risk.
- IT leaders are challenged to deliver increasingly high reliability in complex environments, but many perceive that chaos engineering is too risky.
- Most traditional disaster recovery (DR) programs lack integration with site reliability engineering (SRE) practices, resulting in decreased IT resiliency and suboptimal reliability.

Recommendations

I&O leaders responsible for agile and DevOps initiatives — in partnership with application leaders — must:

- Remove constraints to product delivery and streamline the delivery life cycle by adopting a DevOps value stream management platform (VSMP) and a DevOps value stream delivery platform (VSDP).
- Accelerate delivery of customer value and reduce risk by implementing continuous compliance automation (CCA) tools.
- Deliver higher reliability by embracing chaos engineering as a regular product team activity.
- Iteratively improve IT resiliency and reliability by instituting IT resilience roles and by using automation, monitoring and alerting tools as part of SRE efforts.

Strategic Planning Assumption(s)

By 2023, 70% of organizations will use value stream management to improve flow in the DevOps pipeline, leading to faster delivery of customer value.

By 2023, the use of value stream delivery platforms to streamline application delivery will grow from 10% to 40%.

By 2023, 60% of organizations in regulated verticals will have integrated continuous compliance automation into their DevOps toolchains, improving their lead time by at least 20%.

By 2025, 60% of I&O leaders will implement chaos engineering to add resilience and velocity improvements to value stream flow, increasing system availability by 10%.

Through 2025, 20% of enterprises will go beyond SRE by adding IT resilience roles to improve resiliency posture between product teams and traditional DR.

Analysis

What You Need to Know

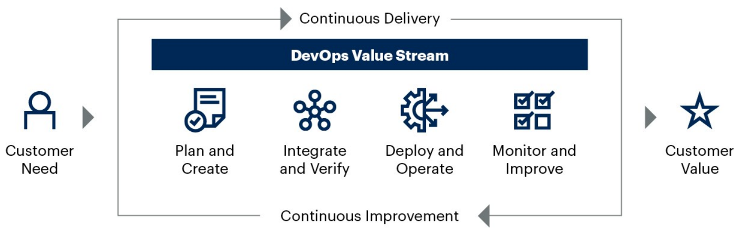
DevOps practices improve the flow of customer value via agile delivery methods, collaboration and automation. Agile and DevOps practices require organizations to build a collaborative culture where development, operations and other IT and business stakeholders work together to improve and accelerate the delivery of value to customers.

DevOps value stream management provides DevOps teams and stakeholders with key insights and metrics to identify, measure and guide their actions. These insights help them to optimize the flow of product increments and value to the customer.

Value stream mapping enables DevOps teams to remove waste, build mutual trust, increase transparency and align their goals with organizational objectives. This "systems thinking" approach helps DevOps teams to expand their focus beyond siloed operational metrics to instead deliver on customer-centric, team-level performance indicators. Continuous feedback and learning are also important aspects of value stream management, as these practices help DevOps teams to identify and remove constraints, thus improving quality, reliability and security. Figure 1 illustrates these key components of the DevOps value stream.

Figure 1: DevOps Value Stream

DevOps Value Stream



Source: Gartner
734377_C

Gartner

> "If you can't describe what you are doing as a value stream, you don't know what you're doing."
>
> — *Karen Martin and Mike Osterling, Value Stream Mapping*

New developments in DevOps tools and processes are transforming the way I&O leaders and DevOps teams can optimize their value stream to deliver customer value faster and more reliably. These developments include:

- **DevOps value stream management platforms (VSMPs).** DevOps teams face challenges to quantifying and improving release velocity, application quality, customer value and organizational effectiveness. They need an orchestration control plane (with both a management and a governance layer) to plan, build, release and monitor activities. DevOps VSMPs enable teams to orchestrate activities by providing visibility and analytics across the entire value stream.

- **Value stream delivery platforms (VSDPs).** DevOps teams are tasked with streamlining their software development and delivery workflows but often struggle to identify and remove constraints to value delivery. DevOps VSDPs provide preintegrated toolchains that enable teams to reduce the overhead of managing complex toolchains while also enhancing visibility, traceability, auditability and observability across the application delivery value stream.

- **Continuous compliance automation (CCA) tools.** Compliance and security practices often depend on manual, traditional methods (such as spreadsheets, checklists and playbooks) that impede agility in value streams. Compliance breaches often occur late in the software development life cycle (SDLC), resulting in costly mistakes that are difficult to correct. Agile and DevOps initiatives demand a layered approach to integrated security via collaboration with information security teams. As organizations face an increasing number of regulatory obligations, automating compliance and security processes with CCA tools will become even more essential for I&O leaders and DevOps teams.

- **Chaos engineering.** Reliability is table stakes in digital business. In the Gartner 2019 DevOps survey, 52% of respondents indicated that improved system reliability was one of their the top five objectives for initiating DevOps practices, while 53% indicated that improving release quality was a top-five objective. [1] Many operational efforts to improve reliability are reactive, emphasizing incident management and service restoration. However, this approach fails to prevent future defects and incidents that will impact the organization's reputation. Chaos engineering serves as a preventative approach for organizations to deliver high reliability in complex environments.

- **IT resiliency roles.** Most organizations are terribly ill-prepared for traditional DR, and even those that are ahead of the curve find they lack transparency between DR and product teams to promote effective recovery (much less resilience). The resulting chasm between teams hinders the ability of senior executives to understand relative end-to-end IT resilience and to prioritize areas that need greater investment. The addition of IT resiliency roles enhances collaboration and alignment between DR teams and product teams to deliver better resilience across the DevOps value stream.

Strategic Planning Assumptions

Strategic Planning Assumption: By 2023, 70% of organizations will use value stream management to improve flow in the DevOps pipeline, leading to faster delivery of customer value.

Analysis by: Hassan Ennaciri

Key Findings:

- As organizations expand usage of agile and DevOps, teams find it challenging to detect and remove constraints to product delivery. This hinders their ability to improve velocity, increase quality and optimize value.
- Current DevOps toolchains require manual effort to maintain and integrate stand-alone tools and to orchestrate pipeline workflows, which detracts from value-generating activities.
- Agile and DevOps teams who focus only on technical performance metrics (at the exclusion of customer-value-centric metrics) will fail to align their priorities with the organization.

Market Implications:

DevOps VSMPs help organizations break down silos by connecting multiple tools to support processes across multiple teams. This integrated approach allows organizations to optimize their DevOps operating models, technology and processes. DevOps VSMPs provide product owners, IT leaders and executive leadership with real-time visibility into product delivery flow.

DevOps VSMPs simplify tool integration by providing out-of-the-box connectors to many popular DevOps tools and extensibility through simple integration methods. By integrating tools, DevOps VSMPs provide product teams with end-to-end visibility. As these platforms continue to evolve, they will provide customer-centric metrics and analytics that drive business-aligned product delivery.The following drivers will increase adoption of DevOps VSMPs in the next two to three years:

- Interest in lean optimization of the value stream and application of value stream principles
- Need for a consolidated source of end-to-end metrics
- Demand for customized dashboards and views of product delivery for other stakeholders and leadership
- Desire to correlate financial data, customer satisfaction with product delivery metrics
- Need for better oversight when using service providers or offshore resources for product development
- Increased governance, security and compliance requirements

DevOps VSMP providers continue to expand their capabilities through innovation or acquisitions. Gartner expects other DevOps tool vendors to expand their capabilities to offer VSMPs. As platform capabilities continue to evolve and improve, organizations must use DevOps VSMP platforms to:

- Leverage advanced capabilities, such as change risk analytics, to make more informed decisions about releasing new features.
- Gain a consolidated view of governance, security and compliance across all product lines.
- Provide customized dashboards and views of product delivery for other stakeholders and leadership.
- Apply expanded business outcome metrics to optimize product delivery and meet business goals.

DevOps VSMPs will play a strategic role in organizations and will be used by multiple stakeholders. Since these platforms are still evolving their key capabilities, DevOps teams must collaborate with IT and business stakeholders to ensure the selected vendor provides features that meet the organization’s needs. Gartner cautions against investing in a VSMP for organizations just starting to develop their agile and DevOps practices.

Recommendations:

- Remove impediments in product delivery by investing in a DevOps VSMP that provides consolidated insights into the performance, quality and value of products.

- Minimize toil when integrating tools by leveraging the prebuilt integrations and workflow orchestration capabilities of a VSMP.
- Support business-driven decisions by providing real-time, data-driven metrics and value stream insights.

Related Research:

The Future of DevOpsToolchains Will Involve Maximizing Flow in IT Value Streams

Bust Silos, Focus on Customers and Enhance Business Outcomes Through Value Streams

Analyze Value Stream Metrics to Optimize DevOps Delivery

Market Guide for DevOps Value Stream Management Platforms

Case Study: Manage the DevOps Toolchain as a Product (LexisNexis)

Strategic Planning Assumption: By 2023, the use of value stream delivery platforms to streamline application delivery will grow from 10% to 40%.

Analysis by: Manjunath Bhat

Key Findings:

- Client interest in DevOps VSDP providers is on the rise, as client inquiries about these providers increased by 57% YOY between June 2018 and June 2020.
- Organizations find it difficult to scale their DevOps initiatives because DevOps teams use multiple point solutions. These disparate tools increase complexity due to orchestration, integration and management issues.
- Product teams struggle to reduce the time to market and deliver faster customer value due to constraints and lack of visibility into the flow of work.
- As organizations transition to remote work styles and reduce opex expenditures, platform teams find it challenging to establish scalable, secure access to DevOps environments.

Market Implications:

DevOps VSDPs provide a unified platform to reduce the complexity of integrating pipeline activities while providing visibility to key value stream metrics across the application development value stream. This value stream is composed of a sequence of activities, such as product planning, build automation, continuous integration, test automation, continuous deployment and rollback, release orchestration, and automated security policy enforcement.

The following trends will drive rapid adoption of DevOps VSDPs in the next two to three years:

- Cloud adoption
- Container-native architectures
- Increased use of agile development methodology
- Digital transformation initiatives requiring faster time to market
- Business pressure to show that DevOps creates business value

DevOps VSDP providers continue to enhance and expand their offerings through organic innovations and acquisitions. We expect more consolidation to happen in this market through both organic (expansion of product capabilities) and inorganic innovation (mergers and acquisitions).

Organizations must leverage the capabilities of DevOps VSDP providers as they mature across four key areas:

- Security and compliance automation through shift-left approaches
- Support for pipelines as code, infrastructure as code and policy as code
- Building visibility, traceability, auditability and observability into the software delivery pipeline
- Continuous cost optimization for application deployments in public clouds

Both product and platform teams will use DevOps VSDPs. However, Gartner cautions against the choice of a DevOps VSDP dictating application architecture. For example, some VSDPs only support serverless architectures. This may be exactly what product teams need in some cases, but it is not suited for all types of workloads. Platform teams must be careful not to enforce a standardized DevOps VSDP across all product teams when they are not ready to replace their existing toolchain. A DevOps VSDP must only be implemented when it enables developer productivity and business agility.

Recommendations:

- Scale DevOps initiatives by adopting VSDPs that reduce the overhead of managing complex toolchains and meet the needs of multiple product teams.
- Improve the flow of work by streamlining the application delivery life cycle with VSDPs that provide enhanced visibility, traceability, auditability and observability across the DevOps pipeline.
- Support remote development teams by adopting cloud-based VSDPs and using their integration and collaboration capabilities for code reviews, code sharing and issue tracking.

Related Research:

The Future of DevOpsToolchains Will Involve Maximizing Flow in IT Value Streams

Market Guide for DevOps Value Stream Delivery Platforms

How to Build and Evolve Your DevOps Toolchains

Strategic Planning Assumption: By 2023, 60% of organizations in regulated verticals will have integrated continuous compliance automation into their DevOps toolchains, improving their lead time by at least 20%.

Analysis by: Daniel Betts

Key Findings:

- Agile and DevOps accelerates the pace of digital business, but the constant change to production introduces considerable compliance risks.
- Traditional auditing and compliance checks are often performed manually and are not integrated into value stream workflows, resulting in decreased agility and lost productivity.
- Implementing tools without accounting for security and compliance requirements often causes the risk of audit failure.

Market Implications:

DevOps teams must remove constraints to value streams to deliver services faster and rapidly respond to threats that endanger the enterprise. Traditional implementation methods, such as manual reviews, spreadsheets, checklists and playbooks, are error-prone and restrict value streams flow. Compliance violations detected late in the software development life cycle (SDLC) result in costly mistakes that are difficult to remediate efficiently.

Compliance automation in DevOps toolchains provide organizations with modernized compliance and governance capabilities. CCA tools integrate compliance into all phases of the delivery pipeline and consistently enforce compliance policies without sacrificing operational agility. As organizations face an increasing number of regulatory obligations, CCA will become even more critical to DevOps teams as they strive to maintain delivery velocity.

CCA tools help organizations meet security and compliance requirements at various phases of the application delivery life cycle, maintaining unimpeded flow in value streams through:

- Discovery and detection of compliance violations and vulnerabilities.
- Policy enforcement through application of regulatory compliance templates and automatic enforcement of environment-specific organizational rules and standards through DevOps toolchains.
- Reporting and remediation, enabling reviews that address vulnerabilities, minimize compliance drift and enable continuous improvement.

CCA requires a change in roles and responsibilities, as well as new practices and technologies. It also means that organizations must seek new ways to measure the impact of their CCA initiatives and how they affect their teams. While CCA is becoming increasingly beneficial for I&O leaders and DevOps teams, poor implementation of these solutions will only serve to increase business risk. Organizations must carefully integrate CCA into the DevOps toolchains. DevOps teams must not assume that implementing CCA will automatically result in the delivery of compliant software.

Recommendations:

- Simplify and enforce required regulatory controls in value streams by collaborating with key stakeholders in development, information security, legal, compliance and audit.

- Balance speed and risk by implementing CCA to detect and remediate compliance violations throughout value streams.
- Optimize and secure DevOps toolchains by assessing them against the organization's security and compliance requirements.

Related Research:

Innovation Insight for Continuous Compliance Automation

Market Guide for Compliance Automation Tools in DevOps

3 Steps to Ensure Compliance and Audit Success With DevOps

Strategic Planning Assumption: By 2025, 60% of I&O leaders will implement chaos engineering to add resilience and velocity improvements to value stream flow, increasing system availability by 10%.

Analysis by: Jim Scheibmeir

Key Findings:

- According to Gartner's 2019 Agile in the Enterprise Survey, 32% of respondents indicated that shifting their focus to "do things right, not fast" was one of their top three challenges to successful adoption of agile development. [2]
- In the 2019 Gartner DevOps Survey, more than half of the respondents (52%) identified system reliability as one of their top five objectives for DevOps adoption. However, Gartner predicts that less than 5% of the target audience utilize chaos engineering to improve system reliability.
- Value stream delivery messaging often focuses only on flow and velocity. DevOps teams who do not balance these concerns with practices that improve the reliability of delivered services and systems will undermine their ability to increase release velocity.

Near-Term Flag: Initially, DevOps teams will utilize chaos engineering and value stream management as individual approaches to different concerns (that is, reliability versus flow). As these practices mature, teams will need to combine analysis of both value stream management and chaos engineering to deliver reliability at speed.

Market Implications:

Chaos engineering helps teams build resiliency into their platforms and products by intentionally attacking dependencies to test and improve tolerance. Value stream management and delivery illuminate areas of waste and constraints in delivery but do not necessarily help I&O leaders and DevOps teams build more robust systems. I&O leaders should integrate chaos engineering tools and the resulting insights into their value stream oversight to ensure a balanced focus on both reliability and flow. This practice tagging and the associated visibility helps to drive risk- and value-based discussions about speed to market, which is frequently critical, and the mean time between failures (MTBF) of the service or product, which may warrant new ways of working.

Chaos engineering enables DevOps teams to discover risky knowledge silos, such as how to respond if senior team members leave the organization. Chaos engineering can also help teams understand the quality of their support documentation. For example, chaos engineering can provide insights that help them determine whether following this documentation verbatim during a staged outage will lead to availability, or if a system will further drift into unknown states. Chaos engineering will become increasingly valuable as enterprise systems become more complex (with distributed systems, abstracted services and SaaS integrations) and quickly identifying root causes becomes much more difficult.

Recommendations:

- Adopt a balanced approach to value stream discussions by addressing both velocity and reliability concerns.
- Take a test-first approach to chaos engineering by practicing attack days within the lab environment and isolating from production services.

Related Research:

Innovation Insight for Chaos Engineering

How to Safely Begin Chaos Engineering to Improve Reliability

DevOps Teams Must Use Site Reliability Engineering to Maximize Customer Value

Strategic Planning Assumption: Through 2025, 20% of enterprises will go beyond SRE by adding IT resilience roles to improve resiliency posture between product teams and traditional DR.

Analysis by: Ron Blair

Key Findings:

Traditional IT DR is ill-prepared in terms of its ability to **absorb** or **recover** from hazards:

- Not Redundant: 64% of respondents do not have multisite redundant designs for critical systems, per Gartner's IT Score. [3]
- Cannot Recover: 34% of respondents have had significant problems in recovering from their last disaster, per Gartner's 2019 Global Security and Risk Survey. [4]
- Old School: Only 17% ensure automation of IT DR plans, per Gartner IT Score for Business Continuity Management. [5]
- Low Visibility: Only 13% of respondents have an end-to-end business-services view of most or all technical underpinnings, per Gartner's IT Score.
- Misalignment of Needs: 61% of respondents are merely making educated guesses about resiliency needs, as only 39% carry out cross-functional business impact analysis, per Gartner IT Score for Business Continuity Management. [6]

DevOps teams focus little on **recoverability**, particularly unknown hazards:

- Only 49% of respondents indicated that their DevOps teams have DR controls, and nearly a quarter of those that do are limited to manual approaches, per the 2019 Gartner DevOps Survey.
- "Do things right, not fast" was a top-three most important challenge to making agile development successful for 28% of teams, per Gartner's 2020 Agile in the Enterprise Survey.

Gaps between teams and practices obscure overall IT resilience health:

- Board-level IT resilience committees of leading enterprises are increasingly seeking greater transparency on their true end-to-end resiliency health.
- Organizations with strong SRE and chaos engineering practices are better prepared within their realm, but few SRE teams are integrated with disaster or business continuity teams.
- SRE is only one of 11 cloud operations patterns. Many enterprises often deploy a mix of patterns — from siloed to platform to product-centric — within business units. Each presents additional IT resilience blind spots across the enterprise.

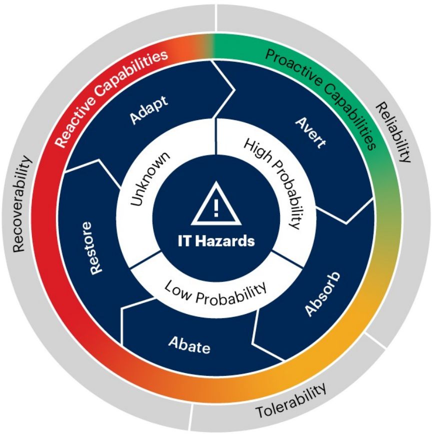
Near-Term Flags: In the last 12 months, Gartner inquiry volume related to "IT resilience" has increased by nearly 50%. Through 2021, interest will continue to grow as a result of recent events (such as COVID-19), a greater proportion of applications being run by DevOps teams, and shifts in regulatory focus toward resilience (for example, requirements in the financial sector like those co-created by The Bank of England [the Bank], Prudential Regulation Authority [PRA] and Financial Conduct Authority [FCA]).

Market Implications:

IT resilience is the organization's ability to anticipate, detect, assimilate and adapt to IT-related hazards — such as application defects, performance thresholds, security vulnerabilities, single points of failure and service provider outages — and to continuously improve capabilities to avert, absorb, abate and recover (see Figure 2).

Figure 2: IT Resilience — Reliable + Tolerant + Recoverable

Gartner's IT Resilience Framework



Source: Gartner

However, most organizations have only an aspirational ability (at best) to accurately assess IT resilience. Resilience posture can be further augmented by DevSecOps practices to appreciably **avert** hazards, and MASA architectures (a mesh architecture of apps, APIs and services) help to further **abate** hazards by decoupling dependencies. SRE practices provide key shift-left approaches for IT resilience, such as:

- Making more systems more stable and reliable by improving capabilities to **absorb** known hazards (hence the usage of error budgets).
- Quickly resolving and abating hazards (hence the focus on measurements like mean time to detect [MTTD] and mean time to recover [MTTR]).

The fourth element, **recover,** is often less pronounced. Blind spots often run rampant between SRE and DevOps teams and traditional IT DR. The ability to **recover** from unknown hazards and potentially cascading failures is imperative for IT resilience. Thus, organizations that are mindful of IT resilience across the enterprise will institute dedicated resiliency roles. These roles help assess and report on IT resilience posture, provide macro indicators (both key performance indicators [KPIs] and key risk indicators [KRIs]) to IT resilience committees, and cascade resiliency requirements.

Recommendations:

Address the traditional IT DR health by:

- Ensuring BIAs are updated, exercise schedules with various scenarios are published, capability gaps are highlighted and formally presented, and decisions are documented.
- Improving traditional IT DR through automation. When doing so, leverage IT resilience orchestration (ITRO) tools to improve time to value. DevOps teams should also use ITRO as an opportunity to advance in-house automation capabilities by leveraging cloud orchestration and configuration automation tools used by DevOps teams.
- Engaging product, DevOps and SRE teams to assess preparedness of applications. Do not assume that applications deemed to be "self-healing" have industrialized recovery plans.

Address IT resilience within DevOps by:

- Instilling the notion among teams that although "always on" is the ideal, the ability to recover is absolutely imperative.
- Establishing essential DR needs by collaborating with stakeholders, including customers and DR/BCP teams, to establish recovery time objectives (RTOs), recovery point objectives (RPOs) and auditing needs (both internal and external).
- Focusing on recovery automation, scenario-based exercises (such as Amazon Web Services [AWS], GameDay or Google DiRT) and increased adoption of chaos engineering and fault injection practices.
- Understanding the degree of dependencies that exist with traditional systems and their respective recovery capabilities and identifying win-win opportunities to help with automation or address technical debt for traditional systems.

Be proactive and iterative by:

- Avoiding a "big bang" IT resilience program. Even with corporate sponsorship, it is likely to fail.
- Choosing a small first-mover team among IT DR, DevOps, platform engineering, DevSecOps and risk management to focus initial efforts on potential blind spots that will yield the best value.

Related Research:

Market Guide for IT Resilience Orchestration

Comparing Cloud Operations Approaches

SRE and DevOps: Fostering End-to-End Accountability Across Teams

Top 3 Trends in Application Architecture That Enable Digital Business

Adopt an Iterative Approach to Drive DevOps Success in Large Organizations

A Look Back

This topic area is too new to have on-target or missed predictions.

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

Evidence

[1] The 2019 Gartner DevOps Survey was conducted to assess the objectives, performance and challenges faced in DevOps initiatives. It also delves into the performance, drivers and challenges of scaling DevOps. The primary research was conducted online from 14 November 2018 through 18 December 2018 among 273 respondents in North America, Western Europe and Asia/Pacific.

Qualifying organizations span various industries except "services." Companies were screened for having annual revenue for fiscal year 2017 to be greater than or equal to $100 million and to have a minimum 50 full-time IT employees. Companies were required to have DevOps to support systems/IT products in production. DevOps efforts were required to be completely in-house or a mix of in-house and outsourcing with a minimum of five DevOps teams to support systems/IT products in production. The sample represents organizations in the U.S. (n = 83), Canada (n = 35), the U.K. (n = 44), Germany (n = 31), India (n = 48) and Australia/New Zealand (n = 32).

Respondents were required to have a role that is primarily IT-focused or that is a fairly even blend of business and IT. They were also required to have involvement in decisions regarding DevOps efforts at their organization. Quotas were applied for countries, industries and annual revenue. The study was developed collaboratively by Gartner Analysts and the Primary Research Team.

[2] Gartner's 2019 Agile in the Enterprise survey was conducted via an online survey from 3 June — 25 June 2019 with 130 Gartner Research Circle Members, a Gartner-managed panel of IT and IT-business professionals. Qualified participants included business end users with either an IT or IT-business focus as a primary role. Eighty-seven percent of participants use agile for at least some of their application development. The survey was developed collaboratively by a team of Gartner analysts and was reviewed, tested and administered by Gartner's Research Data and Analytics team in collaboration with Gartner analysts.

[3] Based on 3456 responses via IT Score for Infrastructure and Operations as of 2Q18.

[4] The Gartner 2019 Global Security and Risk survey was conducted online between March and April 2019 among 698 respondents in the following countries: Brazil (n = 138), Germany (n = 135), India (n = 140), the U.S. (n = 142) and the U.K. (n = 143). Qualifying organizations had at least 100 employees and $50 million in total annual revenue for fiscal year 2018. All industry segments qualified, with the exception of agriculture, construction, IT services, and software and IT hardware manufacturing.

To answer each of the four technology-focused sections of the questionnaire (risk and security management, business continuity management, security compliance and audit management, and privacy), respondents were required to have certain job roles/categories and to have at least some involvement or responsibility with at least one of the technology domains we explored.

Interviews were conducted online and in native languages. The sample was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets, and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

[5] Based on 393 responses via IT Score for Business Continuity Management from 29 April 2019 through 11 May 2020.

[6] Based on 403 responses via IT Score for Business Continuity Management from 29 April 2019 through 11 May 2020.