eGuide

FOUNDRY Formerly IDG Communications is CIO COMPUTERWORLD CSO InfoWorld ITWORLD NETWORKWORLD

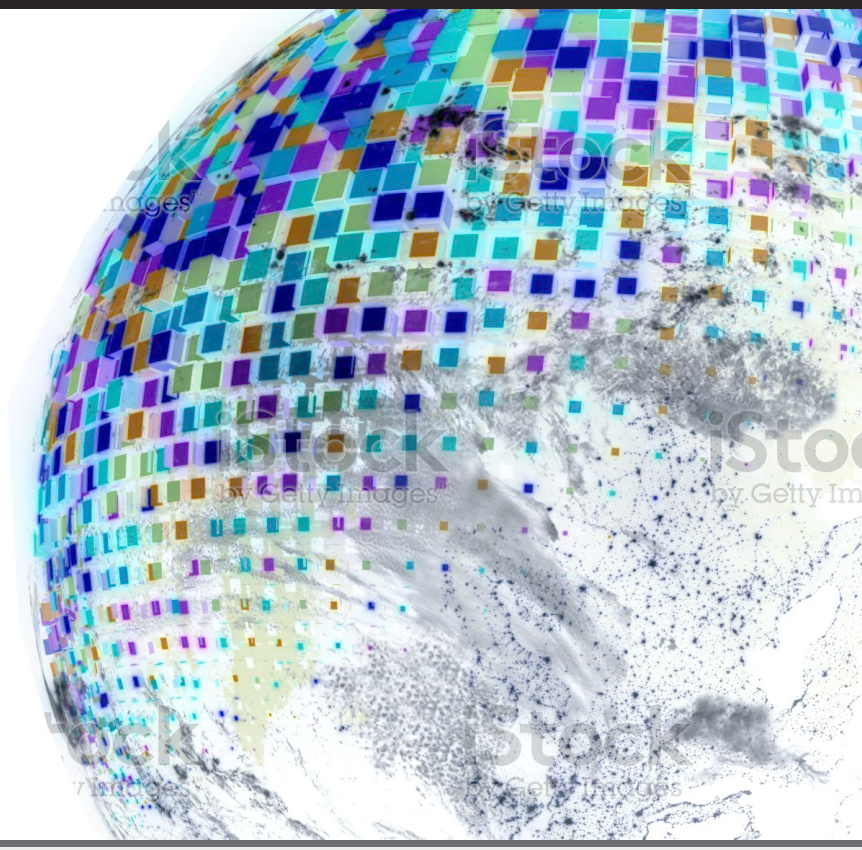
MICRO FOCUS®

presents

Digital transformation: Making it real

How many times have you heard the phrase "digital transformation" over the past several months? What does it really mean, beyond moving operations to the cloud? How can you ensure that your organization's resources—financial as well as human—will be used to maximum benefit?

This eGuide will help you ensure that your brand of digital transformation goes beyond the buzzwords.



Seven tell-tale signs of fake agile

Embracing agile principles doesn't automatically lead to better project management and software development. Here's what separates true agile practitioners from imposters.

BY JOHN EDWARDS | If it looks like a duck, swims like a duck, and quacks like a duck, then it's probably a duck. The same is not true, sadly, for many agile project management and development initiatives.

Too often, an organization may launch something that looks like an agile program, calls itself an agile program, and claims to operate like an agile program, yet really isn't an agile program in the least.

Could your organization be fooling itself into believing that its agile practices and methodologies are the real deal? Read on to see how to detect the seven telltale signs of fake agile in enterprise IT today.

#1. Ignorance

CIOs with inadequate knowledge of agile, including its basic principles, requirements, and benefits, are almost certain to encounter fake agile in practice in their enterprises. Organizations that want to be agile, but are at complete odds with the agile philosophy, can also be fooling themselves about their agile practices, observes Jenny Herald, vice president of evangelism at Gtmhub, a provider of tools for setting and measuring enterprise goals and results.

Along with a well-defined strategy, the best way to prevent fake agile is to make sure agile is actually the right fit. Agile is often viewed as a cure-all, but the reality is that it's not a good fit for all organizations. It requires a mindset shift, Herald notes. "The shift is not just about transitioning to a new set of practices—there must be a change in attitude and mindset around agile values and principles."

Agile success starts at the top. "A CIO needs to ensure there's leadership commitment, and not just from themselves but from leaders across the C-suite and the company as a whole," Herald says. "Leaders must be committed to the enablement of agile teams."

#2. Losing the forest for the trees

When the focus shifts to granular facets of agile, like Scrum ceremonies, instead of actual content and context, agile's true principles are lost, says Prashant Kelker, lead partner for digital sourcing and solutions, Americas, at global technology research and advisory firm ISG.

Agility is about shipping as well as development. By way of example: "Developing software using agile methodologies is not really working if one ships only twice a year," Kelker warns. "Agility works through frequent feedback from the market, be it internal or external."

Too often organizations focus on going through the motions without an eye toward achieving business results. Agility is not only about adhering to a methodology or implementing particular

Agility is not only about adhering to a methodology or implementing particular technologies; it's also about business goals and value realization.

technologies; it's also about business goals and value realization. "Insist on key results every six months that are aligned to business goals," Kelker says.

#3. Team leadership void

When a team lacks a dedicated product owner and/or Scrum master, it will struggle to implement the consistent agile practices needed to continuously improve and meet predictable delivery goals.

CIOs need to ensure they have dedicated team members, and that the product owner and Scrum master thoroughly understand their roles. "If not, make sure they receive some training and, if possible, arrange for an agile coach to provide guidance," advises Jerry Walker, consulting director at software development advisory firm Nexient.

Walker suggests spending time with team members to view and understand how they operate. "Ask to see their team metrics," he says. KPIs can be a good measure of agile success. Are the user stories well written and correctly sized? How good is the acceptance criteria?

#4. Forgoing feedback

Of course, metrics can also be misleading, depending on their use. One of the clearest signs of fake agile, for example, is when an IT department concentrates on team productivity KPIs rather than on value and predictable delivery accompanying each release.

If a CIO recognizes that the IT department is siloed in business goals and objectives, this is fake agile, states Patrick Guidon-Slater, director of agile transformation services for IT service management company TEKsystems. "Agile requires two-way communication, meaning that the IT department and CIO must receive and implement feedback from the customer while also

SHUTTERSTOCK / PATHDOC

sharing updates and developments," he explains.

A CIO should also quickly integrate fresh feedback, deliver value, and then move forward to the next value-measured priority, Guidon-Slater recommends. "This can be accomplished by listening to the concerns of internal stakeholders, providing customer feedback, and ensuring that product backlog priority is aligned

with the enterprise's strategic objectives, product roadmaps, and a well-defined portfolio vision."

#5. Rigidity

Fake agile can also appear when an organization overemphasizes doing agile "correctly." Real agilists focus on being agile, not blindly following accepted protocols to the ultimate degree, says Troy Frever, vice president of engineering at project management software firm LiquidPlanner.

Rigid rules frequently lead to ossified processes and an overall lack of agility. "If there are lots of hard and fast rules, no room for customizing to fit the context, and a 'my way or the highway' attitude, then there's a good chance it's not the real thing," Frever says. Agile should be primarily focused on learning, feedback loops, and responding to change. "If you don't see those things happening, something is likely wrong," he warns.

Hire experienced trainers with great references who understand agile deeply and are also good at teaching it, Frever advises. "Understand that real agility involves a fundamentally different way of working, and get buy-in from both the sponsors and the work teams." Don't expect the transformation to occur overnight. "After training, hire experienced coaches and/or Scrum masters that can nurture new agile teams and help them grow over time," he says.

#6. Talking the talk—and overlooking the tech

CIOs should suspect that something's wrong when teams begin devoting more time to agile catchphrases and events than on improving customer value and experience. Enthusiasm is a powerful team motivator, but leaders need to ensure that zeal doesn't obscure the fundamental mission.

CIOs should coach agile teams on what's important to the organization and its clients and shift the conversation from how software is developed to obtaining feedback on the software itself, says Wing To, vice president of engineering at DevOps platform provider Digital.ai. "Reviews too often focus on checking if something is delivered, or how it was delivered, rather than checking if it's iteratively moving towards strategic goals and delivering what users want," he notes.

Agile's language and processes provide a strong and necessary foundation, To says. Yet, whenever possible, organizations should also equip their agile teams with tools designed to simplify or accelerate activities. Such products and services "are essential to enable teams to focus on the customer value and feedback," he explains.

To also recommends using automation to streamline the delivery of quality software. "For larger enterprises, tools need to be in place to facilitate planning and adapting plans across multiple teams," he adds.

#7. Feeble commitment

Fake agile is frequently rooted in a lack of organizational support. Weak commitment can include a lack of understanding, missing or reluctant buy-in from senior management, or a desire to cut corners simply to save time and money. It can also be identified by a lack of collaboration, poor customer engagement, and a focus on processes rather than outcomes, says Gregory Lenzo, CFO at IBR, a personal and student loan provider.

When a project is afflicted with fake agile, the CIO should first attempt to identify the root cause of the problem, Lenzo suggests. Once the issue has been clearly identified, the CIO can then begin taking steps to resolve the problem. "This may include educating employees on agile [techniques], getting senior management to buy in, and emphasizing the importance of collaboration and customer engagement," he explains.

Three application modernization mistakes to avoid

Using application modernization to pursue cloud-native development at all costs or to gain portability and avoid vendor lock-in are expensive decisions.

BY DAVID LINTHICUM | Application modernization takes existing applications and data sets that run businesses and makes them more useful, productive, and attractive. As I've stated before, some see application modernization as "putting lipstick on a pig," but it should not just make applications appear modern, it should make them look and be modern.

To that end, I see several mistakes being made that will have to be fixed at some point in the future. My advice to friends, colleagues, and clients: You really want to do this only once. Don't get something wrong the first time and then have to fix it down the line.

The trouble is, most people don't believe they will have to fix things in the future, and they make honest mistakes. They don't understand the underlying value of app modernization and how it can be focused incorrectly.

Here are my top three application modernization mistakes in terms of applications that are migrating to the cloud or being modernized once there:

Not doing enough. Most applications move to the cloud by just lifting and shifting. Enterprises find an analog for their existing

legacy "as is" platform on a public cloud and move the code and data there. Easy peasy.

This is often sold as the most cost-effective way to move to the cloud, considering that you're doing the bare minimum. Complicating the problem, the cloud providers themselves often promote a lift-and-shift approach so that they get the revenue ASAP.

We've understood for years that applications that are not refactored to take advantage of the native features of a specific cloud provider are not optimized for that cloud platform and thus cost more to run. Issues often arise, including poor performance, poor user experiences, and lack of fundamentals such as native governance and security protections. The result is, you'll have to loop back at some point and fix those applications.

Doing too much. This isn't as big of a problem as not doing enough, but it's still an issue. Those doing application modernization apply the current religion of cloud-native development to all applications—even where there is no clear business case. They are completely rebuilding most or all applications, typically using containers, microservices, and container orchestration to achieve an objective that never really needed to be achieved.

Not all applications need to be rebuilt from the ground up for the cloud. Some need partial refactoring, enough to ensure that the application is optimized for a cloud platform and takes advantage of native services such as security and performance management. However, there is no reason to toss the existing code and rebuild everything if there is no clear business case to go that far—and certainly not for all applications as a matter of policy without technical or business requirements.

Many are spending five times more than they need to for app modernization. You need to find a balance between doing too much and not doing enough.

Focusing too much on portability and avoiding lock-in. Being "cloud agnostic" is a battle cry I hear a lot these days. The principle is sound (avoiding locking an application into a specific cloud provider), but people think they must move heaven and earth to ensure that it does not happen.

This is really another way of doing too much. However, this time you're rebuilding an application from the ground up, typically using containers or least-common-denominator coding schemes to build portable applications that will never, ever move off that one cloud provider—ever.

The reality is that portability and avoiding lock-in should be considered, but unless there is a compelling business case or technology reason for doing major surgery to an application on a cloud provider, you're preparing for a day that will more than likely never come.

Again, you end up spending three to five times the time and the money, as well as increasing risk, to basically develop that application again. The odds are overwhelming that it will never need to move off the current public cloud host; thus, you're wasting money that could be spent in other ways to benefit the business.

I suspect that we're spending about 50% more on application modernization than we need to right now. Time to work a bit smarter. You'll find good uses for that saved money, trust me.

View cloud architecture through a new optimization lens

Just getting a cloud deployment to work is no longer the goal. Focus on new metrics and approaches to build and deploy an optimal solution.

BY DAVID LINTHICUM | As cloud computing architecture comes of age, the ways we define success should mature as well. In 2021, I pointed out that optimizing cloud computing is more of a binary process than an analog one.

What I said then is still true: "There's a lot at stake. Architectures that are underoptimized and costly (cloud architectures) may indeed work, but they may cause the business to lose millions a week while most people are none the wiser. Thirty technologies are used where 12 would have worked better, and not designing for change means that business agility suffers."

Why are most cloud architectures poorly optimized? During the planning and design stages, most cloud architects do what they were taught in cloud architecture courses, or they apply what they read in any number of how-to-cloud references, or they might even adopt the tips they learned from previous cloud architecture projects and mentors. All guide the architect to a series of generic reference models, processes, and technology stacks that should be modified to address an enterprise's unique business needs. This approach consistently results in underoptimized architectures that cost the enterprises more (or much more) money than they should. What's going on?

To answer that question, let's take a step back. What does an optimized cloud architecture actually mean? I defined the process of cloud architecture optimization in October 2020 and included a high-level model to leverage. I even augmented my cloud architecture course to include this concept, which can be seen here.

Next, we need to recognize that the major focus in the past was to get everything to work together, with little regard as to how well it worked or how complex the solution became. The measure of success was "Does it work?" not "How well does it work?"

FREE-PHOTOS

The planning and development phases of a cloud deployment are great places to plan and build in audit and evaluation procedures that will take place post-development to gauge the project's overall ROI.

During development, the team stayed laser-focused on their approaches to cloud architecture, migration, and net-new development, both in the wide (meta cloud architecture) and in the narrow (micro cloud architectures). Now it's less about how you design and deploy your cloud migrations and net-new cloud-native developments, or how you leverage containers, serverless, or other small or large cloud computing solutions. Instead, it's all about how you define your objectives for that solution.

IT and enterprise management in general is getting wise to the fact that a solution that "works" or "seems innovative" does not really tell you why operations cost so much more than forecast. Today we need to audit and evaluate the end state of a cloud solution to provide a clear measure of its success. The planning and development phases of a cloud deployment are great places to plan and build in audit and evaluation procedures that will take place post-development to gauge the project's overall ROI.

This end-to-beginning view will cause some disturbance in the world of those who build and deploy cloud and cloud-related solutions. Most believe their designs and builds are cutting-edge and built with the best possible solutions available at the time. They believe their designs are as optimized as possible. In most instances, they're wrong.

Most cloud solutions implemented during the past 10 years are grossly underoptimized. So much so that if companies did an honest audit of what was deployed versus what should have been deployed, a very different picture of a truly optimized cloud solution would take shape. Perhaps there is too much or not enough use of containers. Or failure to force cloud-native refactoring—or not considering those advantages. Or the new trend that I'm seeing—making multicloud more complex than it needs to be and failing to define common cross-cloud services such as security and operations. In some cases, a solution uses too many common services, but those situations are not as common.

Speaking in generalities, cloud architects apply what they learn from books, videos, articles, and even the ways that I and other pundits report on how technology should be leveraged. The architects define what the business needs, and then they match those needs to the most optimized solutions. That's a good approach.

However, let's say Vendor A has the best native apps available for your financial operations, Vendor B has the best native apps for your CRM needs, and Vendor C has the best native apps for your inventory requirements. Going multicloud to get the best of breed for these three requirements, as well as for dozens of other choices (security, storage, networking, and so forth), may not be in the overall best interests of your enterprise. Each of those choices adds another layer of complexity and cost that can quickly outstrip the added benefits.

This does not mean to cheap out on the technology you use to build your cloud solutions. Just be aware that getting to the most optimized architecture is still more art than science. Sometimes you need to invest in more technology, sometimes less. What's important is to define something that is as close to optimized as it can get.

Today, cloud optimization means we must audit and reevaluate our current cloud solutions and then look at the augmentation of the metrics moving forward. This will not be easy, but consider the potential value returned to the business. In some cases, cloud optimization may even save the business.

When there are cloud solutions in place that work, many staff on Team "It's Good Enough" tend to become one or all of the three wise monkeys: They do not want to hear, see, or speak any evil about the cloud solution they helped deploy or currently operate. Conversely, there always seems to be someone on Team "Wait—It's Costing How Much?" who realizes the cloud solution will continue to drain enterprise resources much more than it should. They will be the first to suggest or insist on an audit.

Which team will you be on?

NIST's new cyber–resiliency guidance: 3 steps for getting started

The updated guidance provides goals and practical implementation advice, giving organizations a place to start with their cyber–resiliency efforts.

BY CHRIS HUGHES | We're living in a time of unprecedented connectivity. Nearly everything you can think of is already or will soon be connected to networks and the internet. Some metrics rate the broader IoT ecosystem to be over 12 billion devices. At the same time, we are living in a digitally driven economy. Sources such as the World Economic Forum project that soon digital platforms will account for nearly 60% of global GDP. While all this connectivity is great, it isn't without its perils.

Digitally connected systems are vulnerable to myriad cyber-security threats. High-profile security incidents in 2021 included open-source security breaches, alarming vulnerabilities in hyper-scale cloud platforms, and more ransomware attacks. It isn't a matter of if an incident will occur, but when and how systems will both respond and recover from it.

That is why resilience is the name of the game when it comes to modern IT enabled systems. To build on that, NIST has released an updated publication of 800-160 v2, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach." The goal is to apply resilience and system security engineering to develop survivable trustworthy systems. Here are some of the document's core concepts and fundamental takeaways.

BARCIN / GETTY IMAGES

Four fundamental cyber resiliency goals

The guidance is structured around a cyber resilience framework with goals and objectives. By implementing defined cyber resiliency practices, solutions are produced that meet both stakeholder expectations and the goals of the framework. The cyber resilience framework accounts for applying its concepts beyond systems and to business functions, organizations, and even entire industrial sectors.

The publication lays out four fundamental cyber resiliency goals: anticipate, withstand, recover, and adapt. This logical flow of goals emphasizes that it isn't enough to anticipate or withstand adversarial activities against systems; organizations must ultimately improve resiliency by modifying processes, practices, and technologies.

One can't read these goals without thinking of Nassim Taleb's book *Antifragile*, which states: "Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better." Following the goals laid out by NIST, systems would not only resist and recover from shock, but also would iterate and ultimately become even more trustworthy as a result.

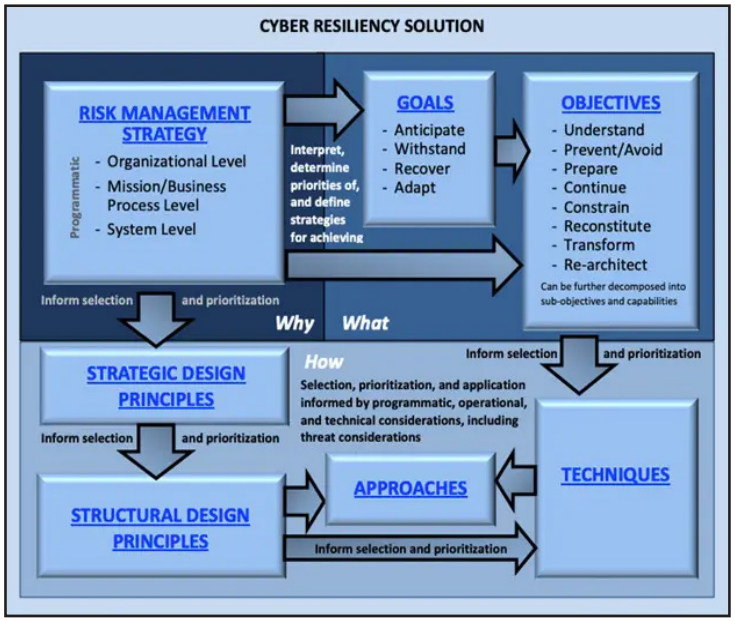
Cyber resiliency objectives

In pursuit of achieving the cyber resiliency goals, specific objectives are defined: *prevent, prepare, continue, constrain*, and *transform*. These objectives collectively look to prevent attacks and incidents from occurring, continue mission/organizational functions when they do happen, limit the damage, and ultimately restore operations and functionality as quickly as possible. Building on that, the goal is to enable critical business functions to handle adversity effectively, be flexible, and most importantly, be sustainable.

Cyber resiliency techniques and properties

NIST defines many techniques and properties in the cyber resiliency framework. Some are aligned with being agile, adaptive, and responsive. Others are aligned with concepts such as deception, non-persistence, and segmentation, which strive to both mislead adversarial actors as well as ensure systems can be sustained through malicious actions and still deliver on supporting organizational business objectives.

As shown in the image below, there is a symbiotic relationship among the components of a comprehensive cyber resiliency solution. All are tied to supporting a defined risk management strategy that cuts across systems, business processes, and the organization itself.



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Following the goals laid out by NIST, systems would not only resist and recover from shock, but also would iterate and ultimately become even more trustworthy as a result.

Cyber resiliency in practice

The guidance goes on to discuss cyber resiliency in practice. It does so by helping organizations develop a tailorable set of resilience concepts, constructs, and practices that can be applied. NIST recognizes that different system types such as IoT, cyber physical systems, and enterprise IT all have unique requirements and therefore demand a unique approach.

There's also a recognition that while cyber resilience techniques can be complementary, they can also be contradictory. For example, segmentation and non-persistence can make monitoring and awareness more difficult. This emphasizes the need for professional practitioner discretion to discern between the application of these techniques based on system and organizational requirements.

Much of what the NIST guidance describes may seem novel or new, and in some cases may warrant additional processes, practices, and technological investments. However, much of what is being proposed can build on existing organizational cybersecurity investments. Most organizations of substantial size and scope likely have investments in areas such as incident response, monitoring, and logging. These investments can be leveraged to complement cyber resilient practices.

The push for building cyber-resilient systems is an iterative process. It involves establishing a baseline, analyzing existing systems and processes, identifying gaps, and providing recommendations to help drive further organizational and mission improvements.

Where to begin with cyber resiliency?

Again, we're living in an increasingly connected society driven by a digital economy. Almost all organizations are becoming technology companies, even if they don't realize it. Those failing to leverage technology to help drive competitive advantage in their respective markets and domains may cease to exist.

That said, these same systems are constantly under a barrage of dynamic threats from threat actors. This reality requires not just using technology but building cyber-resilient systems able to prevent, withstand, and ideally transform in the face of adversity.

Practitioners looking to get started can take a few key steps:

- **Focus on the mission and business functions.** These digital systems are often being wielded to support critical business functions. What are those functions, how do they affect the organization, and why are they of interest to an adversary?
- **Change is the only constant.** The business will constantly change technologies, processes, and objectives. Cybersecurity practitioners must also be flexible and dynamic while applying fundamental cyber resiliency concepts to ensure business continuity and sustainability.
- **Assume a compromise, breach, or incident will occur and likely has already occurred.** The idea of a system being infallible is impractical. Adversaries only need to be right once. Begin by asking yourself and your team, "How do we ensure that when this does occur it isn't so devastating that business and organizational operations grind to a halt? How do we architect our systems in a fashion that allows us to not only absorb challenges, malicious activities, and resistance but thrive in the face of them?"

What is data analytics? Analyzing and managing data for decisions

Data analytics is a discipline focused on extracting insights from data, including collection, analysis, organization, and storage of data, as well as the tools and techniques to do so.

BY THOR OLAVSRUD | Data analytics has become increasingly important in the enterprise as a means for analyzing and shaping business processes and improving decision-making and business results. Its chief aim is to apply statistical analysis and technologies on the data to find trends and solve problems.

Data analytics draws from a range of disciplines—including computer programming, mathematics, and statistics—to perform analysis on data in an effort to describe, predict, and improve performance. To ensure robust analysis, data analytics teams leverage a range of data management techniques, including data mining, data cleansing, data transformation, data modeling, and more.

What are the four types of data analytics?

Analytics breaks down broadly into four types: descriptive analytics, which attempts to describe what has transpired at a particular point in time; diagnostic analytics, which assesses why something has happened; predictive analytics, which ascertains the likelihood of something happening in the future; and prescriptive analytics, which provides recommended actions to take to achieve a desired outcome.

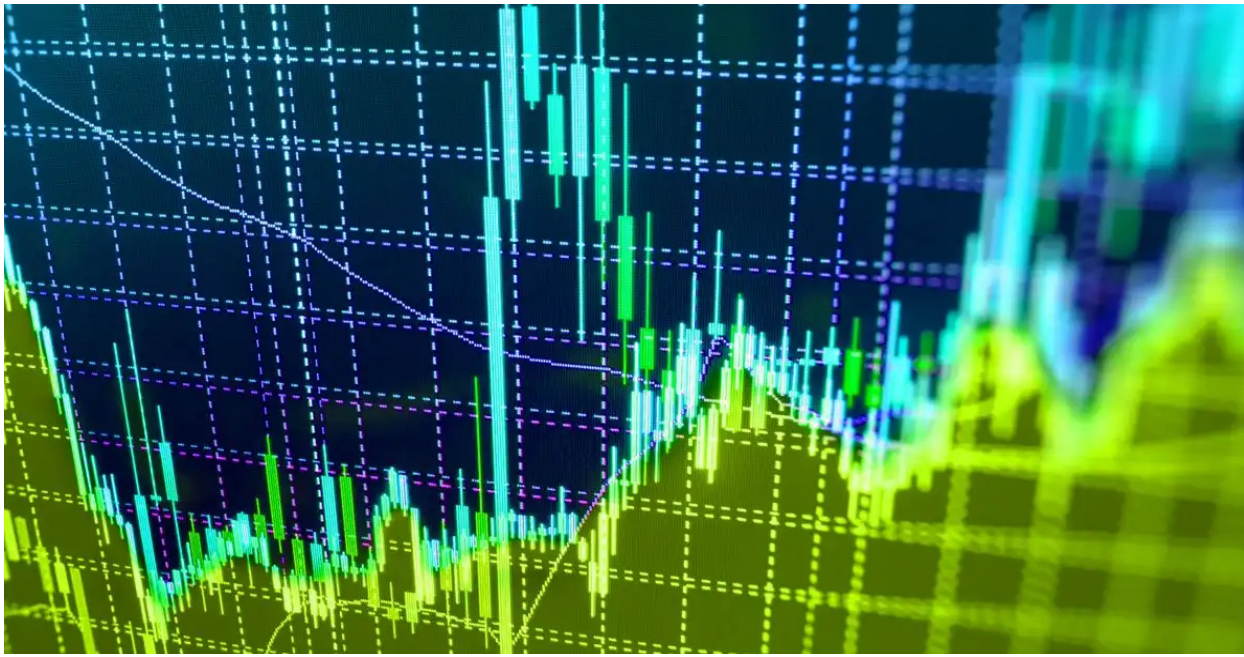
More specifically:

- **Descriptive analytics** uses historical and current data from multiple sources to describe the present state, or a specified historical state, by identifying trends and patterns. In business analytics, this is the purview of business intelligence (BI).
- **Diagnostic analytics** uses data (often generated via descriptive analytics) to discover the factors or reasons for past performance.
- **Predictive analytics** applies techniques such as statistical modeling, forecasting, and machine learning to the output of descriptive and diagnostic analytics to make predictions about future outcomes. Predictive analytics is often considered a type of "advanced analytics," and frequently depends on machine learning and/or deep learning.
- **Prescriptive analytics** is a type of advanced analytics that involves the application of testing and other techniques to recommend specific solutions that will deliver desired outcomes. In business, predictive analytics uses machine learning, business rules, and algorithms.

Data analytics methods and techniques

Data analysts use a number of methods and techniques to analyze data. According to Emily Stevens, managing editor at CareerFoundry, seven of the most popular include:

- **Regression analysis.** Regression analysis is a set of statistical processes used to estimate the relationships between variables to determine how changes to one or more variables might affect another. For example, how might social media spending affect sales?
- **Monte Carlo simulation.** According to Investopedia, "Monte Carlo simulations are used to model the probability of different outcomes in a process that cannot easily be predicted due to the intervention of random variables." It is frequently used for risk analysis.
- **Factor analysis.** Factor analysis is a statistical method for taking a massive data set and reducing it to a smaller, more manageable one. This has the added benefit of often uncovering hidden patterns. In a business setting, factor analysis is often used to explore things like customer loyalty.
- **Cohort analysis.** Cohort analysis is used to break a dataset down into groups that share common characteristics, or cohorts, for analysis. This is often used to understand customer segments.
- **Cluster analysis.** StatisticsSolutions defines cluster analysis as "a class of techniques that are used to classify objects or cases into relative groups called clusters." It can be used to reveal structures in data — insurance firms might use cluster analysis to investigate why certain locations are associated with particular insurance claims, for instance.
- **Time series analysis.** StatisticsSolutions defines time series analysis as "a statistical technique that deals with time series data, or trend analysis. Time series data means that data is in a series of particular time periods or intervals." Time series analysis can be used to identify trends and cycles over time, e.g., weekly sales numbers. It is frequently used for economic and sales forecasting.
- **Sentiment analysis.** Sentiment analysis uses tools such as natural language processing, text analysis, computational linguistics, and so on, to understand the feelings expressed in the data. While the previous six methods seek to analyze quantitative data (data that can be measured), sentiment analysis seeks to interpret and classify qualitative data by organizing it into themes. It is often used to understand how customers feel about a brand, product, or service.



THINKSTOCK

Data analytics tools

Data analysts and others who work with analytics use a range of tools to aid them in their roles. The following are some of the most popular:

- **Apache Spark.** An open-source data science platform for processing big data and creating cluster computing engines.
- **Excel.** Microsoft's spreadsheet software is perhaps the most widely used analytics tool, especially for mathematical analysis and tabular reporting.
- **Looker.** Google's data analytics and BI platform.
- **Power BI.** Microsoft's data visualization and analysis tool for creating and distributing reports and dashboards.
- **Python.** An open-source programming language that helps users extract, summarize, and visualize data.
- **Qlik.** A suite of data analytics, data integration, and programming platforms for exploring data and creating data visualizations.
- **QuickSight.** A BI and analytics cloud service from Amazon designed to integrate with cloud data sources.
- **R.** An open-source data analytics tool for statistical analysis and graphical modeling.
- **RapidMiner.** A data science platform that includes a visual workflow designer.
- **SAS.** An analytics platform for business intelligence and data mining.
- **Sisense.** A popular self-service business intelligence platform.
- **Tableau.** Data analysis software from Salesforce for creating dashboards, maps, and visualizations from data.
- **Talend.** A platform for big data file transformations and loading used by data engineers, data architects, analysts, and developers.

Data analytics vs. data science

Data analytics and data science are closely related. Data analytics is a component of data science, used to understand what an organization's data looks like. Generally, the output of data analytics are reports and visualizations. Data science takes the output of analytics to study and solve problems.

The difference between data analytics and data science is often seen as one of timescale. Data analytics describes the current or historical state of reality, whereas data science uses that data to predict and/or understand the future.

Data analytics vs. data analysis

While the terms data analytics and data analysis are frequently used interchangeably, data analysis is a subset of data analytics concerned with examining, cleansing, transforming, and modeling data to derive conclusions. Data analytics includes the tools and techniques used to perform data analysis.

Data analytics vs. business analytics

Business analytics is another subset of data analytics. Business analytics uses data analytics techniques, including data mining, statistical analysis, and predictive modeling, to drive better business decisions. Gartner defines business analytics as "solutions used to build analysis models and simulations to create scenarios, understand realities, and predict future states."

Data analytics examples

Organizations across all industries leverage data analytics to improve operations, increase revenue, and facilitate digital transformations. Here are three examples:

UPS delivers resilience, flexibility with predictive analytics. Multinational shipping company UPS has created the Harmonized Enterprise Analytics Tool (HEAT) to help it capture and analyze customer data, operational data, and planning data to track the real-time status of every package as it moves across its network. The tool helps it keep track of the roughly 21 million packages it delivers every day.

Predictive analytics helps Owens Corning develop turbine blades. Manufacturer Owens Corning, with the help of its analytics center of excellence, has used predictive analytics to streamline the process of testing the binders used in the creation of glass fabrics for wind turbine blades. Analytics has helped the company reduce the testing time for any given new material from 10 days to about two hours.

Kaiser Permanente reduces waiting times with analytics. Kaiser Permanente has been using a combination of analytics, machine learning, and AI to overhaul the data operations of its 39 hospitals and more than 700 medical offices in the US since 2015. It uses analytics to better anticipate and resolve potential bottlenecks, enabling it to provide better patient care while improving the efficiency of daily operations.

Data analytics salaries

Here are some of the most popular job titles related to data analytics and the average salary for each position, according to data from PayScale.

- Analytics manager: ..... $71K-$131K
- Business analyst: ..... $47K-$84K
- Business analyst, IT: ..... $51K-$100K
- Business intelligence analyst: ..... $52K-$97K
- Data analyst: ..... $45K-$87K
- Market research analyst: ..... $41K-$77K
- Operations research analyst: ..... $47K-$117K
- Quantitative analyst: ..... $60K-$132K
- Senior business analyst: ..... $65K-$117K
- Statistician: ..... $55K-$118K

Give your analytics career a boost with big data and data analytics certifications.

About Micro Focus

Micro Focus is one of the world's largest enterprise software providers. They help customers embrace balancing today's IT needs with transforming for tomorrow's digital opportunities. Their mission-critical solutions, strategic services and support, and partner network help thousands of customers worldwide manage and evolve the core IT elements of their business. These solutions extend across the enterprise—including security, IT operations, application delivery, governance, modernization, and analytics. By embracing the dilemmas of digital transformation their customers can solve how to run and transform at the same time.

To find out more, visit **www.microfocus.com**.

MICRO FOCUS®