ConductorOne

Why Completeness and Accuracy Are Important

Many businesses rely on data-driven workflows, reports, audits, and third-party integrations in their daily operations. In particular, modern, cloud-forward businesses rely on third-party integrations for things as essential to operational security as authentication and access control. However, the effectiveness of these processes hinges on the quality of the underlying data, which must be complete and accurate. When data fails to meet these standards, it can lead to various challenges, including compromised reporting integrity and heightened security risks.

This article introduces the concepts of completeness and accuracy in data-driven workflows like auditing, reporting, and integrations. You'll explore why these standards matter and what can go wrong when your data is incomplete or inaccurate.

What are completeness and accuracy?

Before delving into why they matter, it's first important to understand what the terms completeness and accuracy mean in the context of data. Simply put, completeness denotes that all relevant information is present, while accuracy indicates that the included information is correct. The specifics of these assertions will vary depending on the context in which they are considered.

For instance, in an audit or report, completeness would require that the report capture all relevant data, while accuracy would require that the information be correct as of the report's date and that any calculations included are computed correctly.

In the context of third-party application integrations, completeness would similarly require that all data points be mirrored from one application to the other. In contrast, accuracy would require that the integration periodically update the data to reduce the potential for data mismatch between the source and the mirror. Consider an instance where you might use an integration to pull a list of users from an external source and give these users access to your CRM. Later, if you want to remove a specific user's access at the source of the integration, you would expect this to be reflected by the consuming side of the application in a timely manner.

While the context of the assertions introduces some nuance to their interpretation, the sentiment remains the same. With an established understanding of these terms, the next question is why they matter.

Why are completeness and accuracy important?

There are many reasons why you would want the data involved with your audits, reports, and integrations to be complete and accurate.

Identifying and mitigating risk

When securing your assets and data from potential security risks, you need a plan. Typically, this plan will be based on data about the business, including but not limited to things like:

→ What software are you running, and where?

→ Who has access, and who needs access to a given asset?

→ What kinds of data do the users and software deal with?

Answering questions like these will help you identify potential risks and form the basis of a mitigation plan. However, your efforts will be compromised if the information you are working with is inaccurate or incomplete. Whether there are applications running that you don't know about or users with access that they don't need, misinformation at this stage will allow potential risks and vulnerabilities to sneak through, setting you up for potential issues down the line.

On the other hand, if you can be sure that you have reliable information, then you have a solid foundation for proactive security measures and will be in a good position to prioritize mitigation efforts based on the assessed likelihood and impact of risks.

Incident response

No matter how good your mitigation measures are, you will eventually have to deal with a security incident. When this happens, the quality of your records will be vital to your efforts to resolve the incident as soon as possible. For instance, if you suspect that a given service is compromised, you will likely want to know which accounts have access. If these records are incomplete or inaccurate, your efforts will be immediately hindered.

Similarly, once a breach is resolved, you'll want to analyze it to understand what happened so that measures can be implemented to prevent it from happening again. This process will also be derailed by incomplete or inaccurate information.

Informed decision-making

Businesses are built one decision at a time. For the people responsible for making these decisions, complete and accurate information can be pivotal in choosing one approach over another. High-quality information provides decision-makers with a reliable basis for understanding risks and opportunities and allows stakeholders to assess the potential impact of their decisions as accurately as possible. If you're well-informed, you can also evaluate alternative options and their associated risk factors.

Analyzing past incidents and current threats often provides significant input into the decision-making process. This information must be as accurate and complete as possible, as this will reduce the likelihood of implementing ineffective security measures.

Compliance and regulatory requirements

Many industries, such as finance and healthcare, are subject to compliance and regulatory requirements like SOX and HIPAA. In these cases, completeness and accuracy are paramount in order to ensure compliance. High-quality records can provide evidence of due diligence in compliance and demonstrate a commitment to ethical conduct and corporate governance.

A good compliance posture helps insulate the business against the risk of penalties, fines, and legal liabilities. It also contributes toward a desirable and positive organizational reputation in the eyes of stakeholders.

Credibility and trust

Stakeholder and customer trust in your business should not be taken for granted. If your customers do not trust you, it can be massively damaging to your business. Typically, customers will initially afford you a measure of innate trust. After all, they wouldn't do business with you if they didn't trust you to some extent. However, things can become problematic if you strain this trust by withholding accurate and complete information that is relevant to the customer's privacy, security, or data.

For instance, if you suffer a data breach, the proper thing to do is to inform affected customers in a timely manner, letting them know what happened and what data has been compromised. The information you give them may affect the actions they take to protect themselves from being further compromised. However, suppose you take too long or are vague or incomplete in your reporting of the affected customers and data. When it eventually comes to light, your customers will likely be less forgiving than if you provided them with timely, accurate information. Once this trust is broken, customers will be skeptical of future claims made by the business, and it can take quite some time for this trust to be restored, if it is restored at all.

Consider cases like the 2013 and 2014 Yahoo data breaches, in which billions of user accounts had their data compromised. The extent of these breaches was not revealed to users until years later, by which point any mitigation steps users might have been able to take—like changing passwords—were well and truly too late. In many ways, this is a worst-case scenario, and the damage to the business's reputation was significant.

Third-party integrations

While audits and reports play an important role in business operations, they rarely pose a direct security risk. Third-party integrations, on the other hand, can be quite problematic if not handled with proper care. Integrations can take many forms, but an identity provider (IdP) is one common example.

With an identity provider integration, you essentially pull your list of authorized users from an external source and use this for some kind of access control. This list must be correct and accurate. Consider a case where a user might have access to company applications or assets via a third-party integration. If this user's access is terminated at the source, you would expect it to flow through to any integrated applications. If this is not the case—or even if there is a significant delay between integration syncs—this can pose a risk, as the user may have access you do not want them to have.

The importance of having accurate and complete identity integration is apparent. There are other kinds of integrations that you should also consider, especially data sources that feed into reports and audits. In these cases, outdated or incorrect information at the point of integration will bubble up through the rest of your system, causing the issues previously discussed. As such, ensuring that integrations are as complete and accurate as reasonably possible is in your best interest.

How does ConductorOne ensure completeness and accuracy?

Ensuring that your third-party integrations are complete and accurate is challenging. You likely need to synchronize your application with the source periodically, but the specifics of how often and how to handle updates vary between use cases and different types of applications. Rather than navigating the intricacies of each integration, you might be better off opting for a tool that ensures the completeness and accuracy of these integrations for you.

ConductorOne is an identity and access control solution for modern companies. It offers a unified platform for complete access visibility, just-in-time access, self-service requests, automated user access reviews, and more, essentially managing the lifecycle of access across cloud and on-prem applications and infrastructure and reducing the risk of identity compromise.

Consider a use case like the previously mentioned identity provider integration. In this case, you want the sync to happen in as close to real time as possible. You cannot afford to wait a day or even several hours for changes to propagate, as any time your applications are out of sync, you run the risk of user access being under- or over-provisioned.

ConductorOne mitigates the risk of inaccurate and incomplete integration states by pulling data from integrated applications regularly and continuously. A sync is performed every 1 to 2 hours to ensure your data is mirrored accurately. This kind of problem becomes increasingly complex the more applications you need to consider, and ConductorOne's approach is particularly beneficial for managing a [large collection of integrations, where maintaining up-to-date mirroring is vital for security and operational efficiency.

Wrapping up

In this article, you were introduced to the concepts of completeness and accuracy as they relate to reporting, auditing, and third-party integrations. Data-driven workflows are an essential part of modern businesses. As such, the quality of the data being used is vital. Beyond this, inaccurate or incomplete data, especially in integrations, can worsen your organization's security posture and expose you to unnecessary threats.

If your organization is struggling with cloud-based identity sprawl or unreliable access integrations, ConductorOne—with its comprehensive approach to identity and access control—is the solution you need. Book a demo or take a product tour to see how ConductorOne can boost your integrity and mitigate potential threats.