INSIGHTS FROM THE BDO TECHNOLOGY PRACTICE

Is Your Revenue Platform Ready to Scale Up?

Implementing Controls Over Internally Developed Revenue Systems

BDO

With the increasing popularity of consumption-based revenue models as well as artificial intelligence and machine learning (AI/ML) in customized SaaS and software solutions, financial reporting has grown increasingly reliant on internally developed platforms to provide revenue and customer data.

Complex analytical tools have also emerged to enable users to more easily use the structured and unstructured data generated by these platforms for billing, financial reporting, and other business analyses. As a result, the complexities of these IT environments create additional IT-related risks and internal control considerations that have downstream implications on accounting and financial reporting.

When companies prepare to go public and embark on the journey of Sarbanes-Oxley (SOX) compliance, these financial reporting and billing issues are subject to much greater scrutiny. As they scale up, companies that rely on internally developed revenue systems must ensure they have robust internal controls in place to safeguard against inappropriate user access, unauthorized system changes, and other inaccuracies or misstatements in underlying billing and accounting source data. Their cybersecurity and privacy practices will also gain attention as they pursue and take on larger enterprise customers and those in regulated industries.

THE GROWING IMPORTANCE OF CONTROLS

Complexities and risks around internal systems are evolving, and several emerging issues highlight the growing need for proper internal controls. These include:

An increasing number of SaaS providers generating revenue based on usage transactions conducted using company-developed platforms, external cloud-based platforms, microservices, or other technologies. Often the revenue relies on revenue shares and click-per-action or usage-based fees.

Increasing scrutiny from customers as they seek to verify that usage, billing, or transaction information is accurate and to gain comfort that appropriate technology management, security, and data privacy processes are in place.

Increasing focus from auditors and regulators on whether companies have sufficient internal controls to ensure platform information follows relevant regulations and is subject to sufficient segregation of duties, user access and program change controls, and management analysis.

Failure to adapt to these changing dynamics could introduce significant risks. If internal controls are not up to par, customers may feel they are unable to rely on company-produced data or reporting. Customers may become concerned about the accuracy of billing information, worried about discrepancies that could impact them down the line, or uncertain about the level of security around their information and may elect to look elsewhere to meet their needs.

In the world of SOX, inadequate processes and controls could also result in a material weakness (MW) in internal controls, which indicates that there is a reasonable possibility that a material misstatement of the company's financial statements will not be prevented or detected in a timely fashion. MWs often raise concerns among investors and creditors regarding the credibility of the company's financial reporting.

WHAT TYPES OF BUSINESSES ARE AFFECTED?

These concerns apply across multiple industries and business structures. Any company that transacts via an internal platform and outside of traditional systems, such as Salesforce's, can be impacted. Examples include:

Apps, Software, and SaaS Offerings: These encompass models that follow usage or volume-based revenues or are provisioned electronically through internal company platforms. Fintech and Healthtech companies, for example, frequently use these models.

Marketplaces and Transaction Referral Models: These models refer to companies that receive revenue shares based on the referral of transactions to business partners.

Advertising and Media Companies: Revenue for these companies may depend on factors like clicks and ad views, which may not be represented under the right accounting metrics when tracked internally.

CHALLENGES TO DEVELOPING EFFECTIVE INTERNAL CONTROLS

Companies that rely on internal systems should examine whether their current internal controls can meet their needs and adequately address the level of complexities and risks that exists in these types of IT environments. Those within a company whose role hinges on using and providing accurate reporting data — control owners — must maintain a deep comprehensive understanding of technical platform architecture, data flow, and customer/marketplace interactions in order to properly identify risks and implement the corresponding internal controls.

This process of designing and implementing effective internal controls, however, can prove challenging for certain groups of control owners and stakeholders (e.g., Engineering). Internal platforms are generally the domain of engineering or data teams, rather than finance, accounting, or internal audit. These platforms are highly complex, often involving unstructured data pumped into a data warehouse and likely passing through some form of middleware as well as numerous external SaaS solutions connected by a web of interfaces and microservices managed by one or many code management solutions such as GitHub.

Those control owners on the accounting and finance side of the equation must be able to evaluate each of these components and assess potential impact to financial reporting, but often lack the technical experience required to do so properly. This can make it difficult for them to understand or prepare data flow and system diagrams, identify control gaps, and recommend effective changes. On the other side, while IT and engineering team members do understand these technical complexities — implementing IT-based controls over user access and program changes — building backups to mitigate billing or accounting concerns, frequently takes a backseat to developing and maintaining platform functionality and service availability.

Companies will also need to establish internal controls over their customer-facing services, cloud environments, innovative applications of technology, such as AI, handling personal information, and cybersecurity to manage risks and customer expectations. Industry standards and frameworks including SOC, ISO, and NIST can guide companies with these efforts and help form the foundation for external audits that may become beneficial (or required) to provide assurance to customers, prospects, and business partners.

HOW CAN SAAS COMPANIES DEVELOP SUFFICIENT CONTROLS?

There is no single, one-size-fits-all fix for this issue. Achieving control over the accuracy of platform data may require multiple combined solutions, and criteria will vary depending on companies' unique business models and technical architecture. Technology companies should consider several basic approaches as they work to make improvements, including:

INDUSTRY BENCHMARKING

Companies can leverage independent third-party reports, if available, for sources such as advertising impressions. Reports can be used to compare industry data and trends to their own metrics on figures like revenues or platform volumes. Notable discrepancies could indicate a weakness in internal systems and controls.

PREDICTIVE ANALYSES

Companies can perform analyses of expected transaction volumes and related revenues based on information like historical thresholds, discrete data by customer, and estimations of volume-based revenues based on independent pricing data and transaction volumes. They can also gather data for use in lookback analyses of historical customer credits and differences between expected revenues and actual numbers. For example, in a business-to-business context this would mean requesting that customers explicitly confirm product quantities or volumes invoiced. In consumer-facing businesses, control owners can conduct transactions throughout the year and trace their independent transaction data against the platform's data.

IT GENERAL CONTROLS (ITGCS)

Designing and implementing effective ITGCs, particularly in the areas of user access, program change, computer operations (job monitoring and back-ups), and segregation of duties, are the building blocks of other important system-specific controls. In more heavily regulated industries, like financial technology and healthcare, companies may have already anticipated the need for ITGCs and therefore may be ahead of the game with respect to these measures. Nonetheless all companies should examine the potential impact of any ITGC deficiencies on the validity, completeness, and accuracy of platform data. They should explore whether downstream controls could mitigate those deficiencies and ask how difficult it would be for a user to inappropriately change platform data alone.

RECONCILIATION OF REVENUES TO CASH

Reconciliation involves comparing sales numbers versus cash received during a given period to ensure the numbers line up. However, this measure is only appropriate if revenues are highly correlated to cash in terms of timing and reporting.

RISK ASSESSMENTS

Assessments should involve detailed analyses of any risks in platform data or transaction volumes and pricing. Some examples of considerations that can impact risk include the relative importance of volume-based revenue streams within a business, the likelihood of an error occurring, and the motivations of any employees to misstate sales or financial data — such as incentives, compensation, or opportunities to misappropriate assets.

THIRD-PARTY ATTESTATION

Companies may need to obtain and evaluate SOC 1 or SOC 2 Type 2 reports for service providers that have a key role in transaction processing, financial reporting, and supporting infrastructure, for example. In turn, companies will need to implement technology and process controls to meet business requirements and the expectations of their enterprise customers. They may also require their own third party attestation reports to meet contractual, risk management, and compliance requirements of key customers. This includes SOC 1 for services impacting financial reporting; SOC 2 for areas such as security, availability, and privacy; or ISO 27001 and ISO 27701 to address global security and privacy requirements.

HOW BDO CAN HELP

BDO can help companies evaluate and document data flow and systems diagrams; identify relevant risks and internal controls associated with their unique models and structures; and identify control gaps. With their deep knowledge of industry requirements, our technology and risk advisory professionals can help companies determine specific reporting needs and implement controls that support client needs. We also offer robust third-party attestation services to meet the relevant compliance requirements.

CONTACTS

HANK GALLIGAN
National Technology Industry Leader
hgalligan@bdo.com

MITCH MOULTON
Managing Director, Information Systems Assurance
mmoulton@bdo.com

STEPHANIE HEWLETT
National Technology Assurance Leader
shewlett@bdo.com

MARK LUNDIN
Partner, Third Party Attestation
mlundin@bdo.com

People who know Technology, know BDO.

www.bdo.com/**technology**

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!