KPMG

IT controls and ICFR

Audit Insights

April 2024

The increasing importance of information technology controls in internal control over financial reporting

Information technology (IT) controls play an integral role in ensuring the accuracy, reliability, and security of financial information by enabling organizations to effectively manage risks associated with IT systems and infrastructure. IT controls build trust in financial reporting processes and are an important component of internal control over financial reporting (ICFR).

A recent study conducted by Ideagen Audit Analytics North America sheds light on the significance of IT controls and highlights the most common internal control issues found by auditors in adverse ICFR assessments.[1]

Top 5 issues in adverse ICFR auditor assessments

Rank based on percent of total adverse disclosures referencing issue

Rank	Issue	2018	2019	2020	2021	2022
1	Information technology	35.0%	46.2%	36.2%	42.7%	54.5%
2	Accounting personal resources	44.0%	50.6%	42.1%	48.8%	53.7%
3	Inadequate disclosure controls	19.8%	23.9%	21.7%	24.9%	39.7%
4	Segregation of duties	23.9%	30.4%	19.1%	32.9%	39.3%
5	Nonroutine transactions	11.1%	7.3%	7.2%	13.6%	14.4%

Source: Ideagen, *SOX 404 Disclosures*, 11.

The study reveals that IT concerns have consistently ranked among the top internal control issues in recent reporting years. However, for the first time, IT issues have emerged as the top issue cited in adverse auditor opinions. This shift emphasizes the need for organizations to prioritize IT controls in maintaining the integrity and reliability of financial reporting processes.

Additionally, the study highlights resource constraints and segregation of duties as issues leading to adverse ICFR assessments. These can be correlated to IT issues because an entity may struggle to segregate duties

[1] Ideagen Audit Analytics North America, *SOX 404 Disclosures: A 19-Year Review 2004–2022*, 2022.

within its IT systems when it lacks sufficient resources to manage its organizational needs. This allows management to bypass or override certain IT-enabled controls that can render the IT system ineffective and lead to fraud and errors.

The study further highlights the increasing percentage of adverse ICFR assessments related to first-time filers, with 2021 and 2022 demonstrating the highest rates since the initial years of the Sarbanes-Oxley Act (SOX).

Adverse ICFR increase distribution

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
First Adverse ICFR	62%	39%	83%	66%	37%	29%	33%	31%	32%	31%	39%	31%	31%	27%	32%	42%	61%	53%
New Adverse ICFR	38%	61%	17%	34%	53%	71%	67%	69%	68%	67%	61%	69%	69%	73%	68%	58%	39%	47%

Source: Ideagen, SOX 404 Disclosures, 8.

The increased pace of initial public offering (IPO) activity in 2020 and 2021, when special-purpose acquisition companies became popular, was a likely factor in this trend. When companies react quickly to capitalize on favorable market conditions, they increase their risk of improperly addressing ICFR processes prior to filing.

Which IT control issues drive adverse ICFR results?

IT control deficiencies in ICFR can vary depending on the organization and its specific IT environment, industry, and regulatory requirements. However, certain themes arise more frequently when considering adverse ICFR assessments:

- **Weak access controls over system administration:** Access control issues may include lack of segregation of duties, excessive user privileges, weak password policies for shared service or vendor accounts, inadequate user access monitoring, and untimely access removal when employees or contractors are terminated or transferred. When controls over privileged and administrative user access to financial systems and data are inadequate, it can lead to unauthorized access, data breaches, and fraudulent activities, driving material weaknesses. Inability to properly restrict administrative access can have a pervasive impact on the effectiveness of other internal controls since this super-user level of access can bypass other controls.
- **Inadequate change management:** Poor change management processes can result in unauthorized or untested changes to IT systems that result in errors, data integrity issues, and system failures. In these situations, material weaknesses are often a result of insufficient system access controls when implementing changes (i.e., lack of segregation of duties between development and production access). Utilizing DevOps tools and providing developers with more autonomy in the change release process have led to an increase in change management deficiencies, especially with the continued shift from waterfall to agile methodologies.
- **Inadequate IT governance and oversight:** Weak IT governance and oversight can result in a lack of accountability, unclear roles and responsibilities, and insufficient management oversight of IT controls. This includes issues such as lack of documented policies and procedures, inadequate management review and approval processes, insufficient monitoring and reporting of IT control effectiveness, and failure to remediate identified control deficiencies.
- **Lack of IT training and awareness:** Insufficient training and awareness of IT controls can result in employees failing to properly prioritize IT control implementation, understand their responsibilities, or understand the importance of compliance. A lack of training on IT control policies and procedures,

inadequate communication of control changes, and failure to provide ongoing IT controls awareness training can all have a negative impact on financial reporting.

- **Incomplete identification of systems relevant to financial reporting:** Companies undergoing SOX compliance for the first time or experiencing significant IT transformations can often encounter issues resulting in adverse ICFR results due to unidentified IT systems across the various IT layers (internal or hosted applications, databases, operating systems, networks, and supporting tools). The root cause of such issues is often inadequate investment in time and attention from finance, accounting, and IT organizations to inventory IT systems relevant to ICFR.

How can companies avoid IT control issues?

Conducting a thorough risk assessment can help identify and address weaknesses specific to an organization's IT controls. Consider the following areas for prioritization:

- **Accuracy, completeness, and reliability of data**: Effective controls over IT systems, including applications, data integrity checks, and security measures, help minimize the risk of errors, misstatements, and fraudulent activities. Failures often occur because of inadequate or missing controls to ensure the completeness, accuracy, and reliability of data input through reporting.
- **Data protection and security**: Robust IT controls, such as access controls, privileged access management, and regular system monitoring, are essential to safeguarding sensitive financial information and protecting against unauthorized access and data breaches. In particular, understanding and properly restricting sensitive and privileged access, including maintaining segregation of duties across business and IT functions, is paramount.
- **Transformation impact**: Organizations undergoing transformations need to embed control and security workstreams or activities into their initiatives to ensure compliance, quality, and alignment with changing organizational structures, processes, systems, compliance requirements, and third-party relationships. This can include not only internal processes and systems, but also reliance on third parties and the respective IT control coverage (i.e., SOC 1 reports). It is a leading practice that well-controlled companies embed controls early into their system and process designs and implementations.
- **Compliance with regulatory requirements:** Organizations must establish and maintain effective internal controls, including IT controls, to ensure compliance with regulatory frameworks like SOX and meet the evolving regulatory requirements for cybersecurity and environmental, social, and governance considerations, both in the US and in other jurisdictions where they operate.
- **Efficiency and process optimization:** Well-designed IT controls, including automation, data analytics, generative artificial intelligence (AI), and continuous monitoring tools, can enhance operational efficiency, streamline financial reporting processes, and improve overall control effectiveness. While benefits can be generated through implementation of these optimized approaches, they also bring additional risk and control considerations that should be addressed.
- **Start early:** For organizations preparing for SOX compliance due to an IPO or acquisition, it often takes more than a year to get through the initial SOX compliance effort. It may take even longer if there has not been adequate investment in technology and IT resources. Engaging internal IT and business stakeholders, as well as external resources and auditing specialists where appropriate, is critical.

Conclusion

The importance of IT controls in ICFR is only increasing, particularly as companies navigate an era of compound volatility marked by heightened geopolitical and economic uncertainty and new and emerging risks related to cybersecurity, AI, and generative AI technologies. Organizations must recognize the essential role that IT plays in maintaining accurate financial data and robust internal controls. Importantly, they must regularly assess their IT controls, identifying areas for improvement and implementing measures to mitigate risks swiftly. By prioritizing IT controls during transformations, addressing software and security issues, and ensuring effective segregation of duties, organizations can enhance the reliability, security, compliance, and efficiency of their financial reporting processes.

Contact us

Carly Garrett
Managing Director,
Technology Assurance Audit
KPMG LLP
T: 404-222-7177
E: cgarrett@kpmg.com

Jason Swarts
Managing Director,
Technology Assurance Audit
KPMG LLP
T: 816-802-5658
E: jswarts@kpmg.com

We would like to thank our contributors:
Eric Bloesch, Rebecca Greer, and Sue King.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**