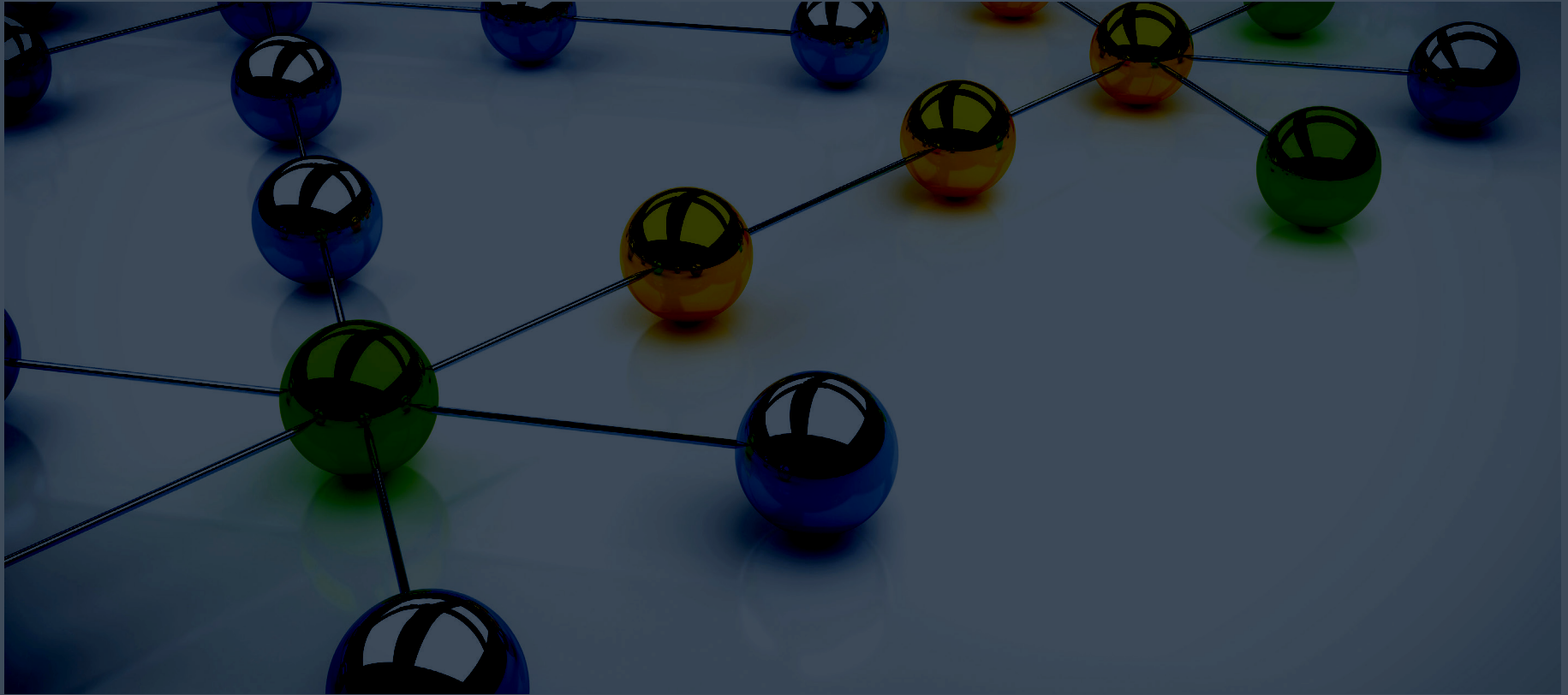




Streamline Information Produced by Entity (IPE): Enhance Audit Data Integrity and Efficiency





Auditors, are you ready to tackle the growing challenges of managing information produced by the entity (IPE)? The Public Company Accounting Oversight Board (PCAOB) is stepping up its scrutiny, and you need to be prepared. The stakes are higher than ever with heightened regulatory focus and evolving PCAOB guidance.

This ebook discusses how to stay ahead of the curve and ensure robust IPE management to maintain data integrity and confidence in your audits.



Understanding the Complexities of IPE

PE includes any data created by the company and used as evidence during audits, whether for testing internal controls or conducting substantive procedures. The increasing use of centralized financial platforms such as SAP and Oracle and technological progress have highlighted the risks of relying on electronic reports and spreadsheets.

For example, a balance sheet review or receivable aging analysis performed using a key report from the ERP application is considered IPE. Verifying the accuracy and completeness of such reports is crucial, similar to confirming a bank statement balance directly with the bank. The Wirecard fraud highlighted the importance of verifying the source of information a company provides to auditors.

The complexity of IPE can vary from system-generated reports to manually prepared spreadsheets and analyses. System-generated reports from standard applications such as SAP's "out of the box" reports are considered lower risk due to their built-in controls and reduced susceptibility to human error. However, manually prepared IPE poses significantly higher risks. Custom queries and complex calculations in Excel require more thorough audit efforts to ensure reliability.

Ensuring the completeness and accuracy of IPE is a crucial yet challenging task for auditors. It demands a deep understanding of data sources, parameters employed, and controls ensuring data integrity. For example, auditors need to understand how user access is granted in the ERP application and the controls in place to prevent unauthorized changes to the data. This challenge intensifies with manually prepared IPE, often characterized by scant documentation, requiring extensive testing to confirm its reliability.



Heightened Regulatory Scrutiny

The PCAOB has intensified its focus on auditors' work. To maintain compliance with PCAOB standards, auditors have imposed stricter documentation requirements on companies concerning IPE. For instance, auditors now require detailed documentation on the source, parameters, and controls for each key report used as audit evidence.

This increased scrutiny means that all evidence the entity produces must be thoroughly documented and verified, adding complexity to the audit process. The PCAOB has issued guidance and inspection findings highlighting deficiencies in how auditors evaluate and test the reliability of IPE, putting pressure on auditors to enhance their validation processes.



How SafePaaS Can Help Auditors

SafePaaS offers several key capabilities that significantly enhance auditors' ability to perform comprehensive and efficient audits, particularly in access governance and controls testing.

Let's examine these features and their advantages:

Standard Out-of-the-Box Reports to gather IPE evidence for identity access, transaction processing, master data management and application configuration controls:

SAFEPAAS PROVIDES AUDITORS WITH PRE-CONFIGURED REPORTS THAT COVER CRITICAL AREAS OF CONCERN:

- **Identity Access:** These reports offer detailed insights into user access rights, roles, and permissions across various systems and applications. Auditors can quickly identify potential access risks, unauthorized privileges, or segregation of duties conflicts.
- **Transaction Processing:** These reports allow auditors to analyze financial and operational transactions, helping detect anomalies, errors, or potential fraud.
- **Master Data Management:** These reports provide visibility into the integrity and consistency of critical business data, enabling auditors to assess data quality and governance practices.
- **Application Configuration Controls:** These reports offer insights into system configurations and changes, helping auditors evaluate the effectiveness of IT general controls (ITGCs).



How SafePaaS Can Help Auditors

- 1. Efficient Evidence Gathering:** These standard reports are readily available control evidence and IPE, significantly reducing the time and effort required for data collection. Auditors can quickly access comprehensive, relevant information without the need for custom report development or manual data extraction.
- 2. Enhanced Audit Quality:** By leveraging these reports, auditors can perform more thorough and accurate assessments of an organization's control environment. The comprehensive nature of the reports allows for deeper insights and more effective risk identification.
- 3. Streamlined Controls:** The reports are designed to align with various regulatory requirements and industry standards, making it easier for auditors to assess compliance with frameworks such as Sarbanes-Oxley (SOX), GDPR, or HIPAA.
- 4. Improved Collaboration:** SafePaaS facilitates better collaboration between auditors and the organizations they audit by providing a centralized platform for accessing and reviewing control evidence.
- 5. SOC Auditor Review:** Thoroughly reviewed by SOC auditors to ensure completeness and accuracy. This review offers additional assurance to auditors who use the platform, improving the reliability and credibility of the generated data and reports.

Advanced Audit Analytics

Beyond standard reports, SafePaaS offers advanced audit analytics capabilities that enable auditors to:

- Perform real-time data analysis for more timely risk identification
- Conduct complex, granular examinations of client data for thorough control testing
- Detect policy violations across various business processes and systems
- Identify discrepancies between approved access requests and actual system access

By using these capabilities, auditors can significantly enhance their audit effectiveness, reduce manual effort, and provide their clients with more valuable insights. The combination of standard reports and advanced analytics empowers auditors to meet the increasing demands of regulatory bodies and adapt to the complexities of modern digital enterprises.

Automating IPE Data Extraction

- **SafePaaS** enables the secure extraction of data from various sources like ERP systems, IDM, and supply chain applications in a usable audit format..
- **SafePaaS** provides pre-built connectors to extract complete audit evidence for systems like SAP, Oracle, Workday, and Microsoft Dynamics. For example, SafePaaS can extract user access details, transaction logs, and configuration settings from the ERP application.
- **SafePaaS** offers flexible subscription options to run one-time scans or continuous monitoring to detect and prevent risks. Auditors can schedule regular scans to monitor changes in user access or configuration settings that could impact the integrity of IPE.



Validating Completeness and Accuracy of IPE

Resolving Data Discrepancies

Example:

Auditors have identified a substantial discrepancy in the user counts between two essential systems: SAP and HCM. This discovery highlights a potential risk in data consistency and system alignment. Here's a breakdown of the situation and an explanation of how SafePaaS can be used to resolve these challenges:

During a routine audit, the team notices:

- SAP system reports 2000 users
- HCM system shows 2200 active users

This 200-user variance raises concerns about data integrity, access control, and potential security risks.

Challenges

1. **Data Inconsistency:** The mismatch in user counts indicates potential issues in user management processes.
2. **Security Risk:** Unauthorized access or orphaned accounts could be present.
3. **Control Concerns:** Discrepancies may lead to compliance issues with internal policies or external regulations.
4. **Audit Efficiency:** Manual reconciliation would be time-consuming and error-prone.

Using SafePaaS for Variance Reconciliation

SafePaaS offers powerful audit analytics to resolve data variance problems efficiently.

- 1. Data Extraction and Consolidation:** SafePaaS can directly extract user data from both SAP and HCM systems, ensuring auditors work with complete and accurate datasets.
- 2. Automated Tie-Out Process:** The platform's analytics tools can automatically compare user listings from both systems, identifying matches and discrepancies without manual effort.
- 3. Variance Analysis:** SafePaaS can categorize and quantify the variances, helping auditors quickly understand the nature of the discrepancies:
 - Newly added users
 - Deactivated accounts
 - Duplicate entries
 - Misclassified user types
- 4. Reconciliation Workflow:** Provides a structured workflow for investigating and documenting each variance:
 - Assign responsibility for each discrepancy
 - Track justifications and resolutions
 - Maintain an audit trail of all actions taken
- 5. Continuous Monitoring:** Enables ongoing monitoring of user counts across systems, alerting auditors to future discrepancies as they occur.

Benefits for Auditors

- **Enhanced Accuracy:** By analyzing 100% of the data, SafePaaS eliminates sampling risks and provides higher assurance.
- **Time Efficiency:** Automated analytics significantly reduce the time required for data comparison and reconciliation.
- **Improved Collaboration:** The platform facilitates discussions between auditors and client management, raising awareness of exceptions or weaknesses.
- **Comprehensive Oversight:** Auditors gain a holistic view of user management across multiple systems, improving their ability to assess overall risk.
- **Evidence Trail:** SafePaaS maintains a clear record of all analyses and justifications, strengthening the audit documentation.

Auditors can efficiently identify, investigate, and resolve data discrepancies. This approach solves the immediate challenge and enhances the overall quality and effectiveness of the audit process.

Enhancing Audit Efficiency

- SafePaaS reduces manual effort and IT dependencies in ERP control testing and reporting by deploying pre-packaged business objects. Auditors can leverage pre-built queries and reports to extract the necessary data, reducing the need for custom programming or scripting ACL.
- This allows auditors to dedicate more time to essential assurance tasks rather than managing IPE populations. SafePaaS offers a centralized platform for overseeing critical reports and spreadsheets, simplifying the process of identifying and examining IPE.
- The platform allows audit teams to focus on value-added activities like testing the accuracy and completeness of IPE. SafePaaS frees up auditors' time to focus on higher-level analysis and risk assessment by automating data extraction and providing visibility into the IPE environment.

Addressing Evolving Regulatory Requirements

- **SafePaaS** assists auditors in staying updated with the changing PCAOB guidelines and SEC disclosure rules related to IPE. The platform offers a structured approach to documenting each IPE component's origin, parameters, and controls to ensure compliance with regulatory standards.
- **SafePaaS** offers advanced analytics capabilities for effectively auditing digital platforms and extracting insights from large datasets. Auditors can use machine learning algorithms to uncover anomalies and patterns in IPE, improving their ability to identify potential issues.
- **The platform boosts auditors' productivity**, ensures quality, and enhances the audit process for digital enterprises. SafePaaS facilitates collaboration and knowledge-sharing among audit teams by providing a centralized platform for managing IPE, ultimately improving overall audit effectiveness.



Key Takeaways

1. Implement automated IPE data extraction tools to streamline the process and ensure audit data completeness and accuracy.
2. Document detailed information about the source, parameters, and controls for each key report used as audit evidence to comply with heightened regulatory scrutiny.
3. Validate the completeness and accuracy of IPE by applying advanced analytics techniques for variance analysis and tie-out across multiple sources.
4. Use pre-built queries and reports to reduce manual effort and IT reliance on ERP control testing and reporting, enhancing audit efficiency.
5. Schedule regular scans to monitor changes in user access or configuration settings that could impact the integrity of IPE.

By automating IPE data extraction, validating completeness and accuracy, enhancing efficiency, and addressing regulatory requirements, SafePaaS enables auditors to overcome key challenges in managing IPE and performing effective audits in the digital age.

To learn more about how SafePaaS can help you streamline IPE, please contact:

Emma Kelly
Senior Marketing Manager
emma.kelly@safepaas.com

3300, Dallas Parkway, Suite 200, Plano, Texas, 75093 USA