The SOCial Hour

IPE Fundamentals for SOC Examinations

forvis mazars

IPE Fundamentals for SOC Examinations

Meet the Presenters

Karen Cardillo
Managing Director, SOC & HITRUST

336.259.6611
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal, SOC & HITRUST

828.989.3176
ryan.boggs@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Agenda

1. What IPE Is & Why It Matters
2. How Auditors Evaluate IPE in SOC Examinations
3. Common IPE Breakdowns in SOC 1 & SOC 2
4. Practical Ways to Improve IPE Reliability
5. SOC 1 & SOC 2 Examples
6. Key Takeaways & Q&A

© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals

IPE Fundamentals

What Is Information Produced by the Entity (IPE)?

IPE includes reports, listings, logs, dashboards, screenshots, and data extracts generated by an organization's systems.

IPE is commonly used to operate controls and support SOC examination testing.

Because it is often produced outside the audit process, its importance is frequently underestimated.

© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals

Why IPE Is Foundational to SOC Examinations

- SOC examinations rely heavily on information produced by management rather than direct observation by the auditor.
- Auditors frequently evaluate control performance using reports, listings, and system-generated data.
- Even when controls are properly designed and executed, unreliable IPE can undermine audit conclusions.
- Incomplete, inaccurate, or poorly controlled IPE may prevent auditors from placing reliance on the evidence.
- When IPE cannot be relied upon, auditors may need to expand testing, request additional evidence, or conclude that controls did not operate effectively.

© 2026 Forvis Mazars, LLP. All rights reserved.

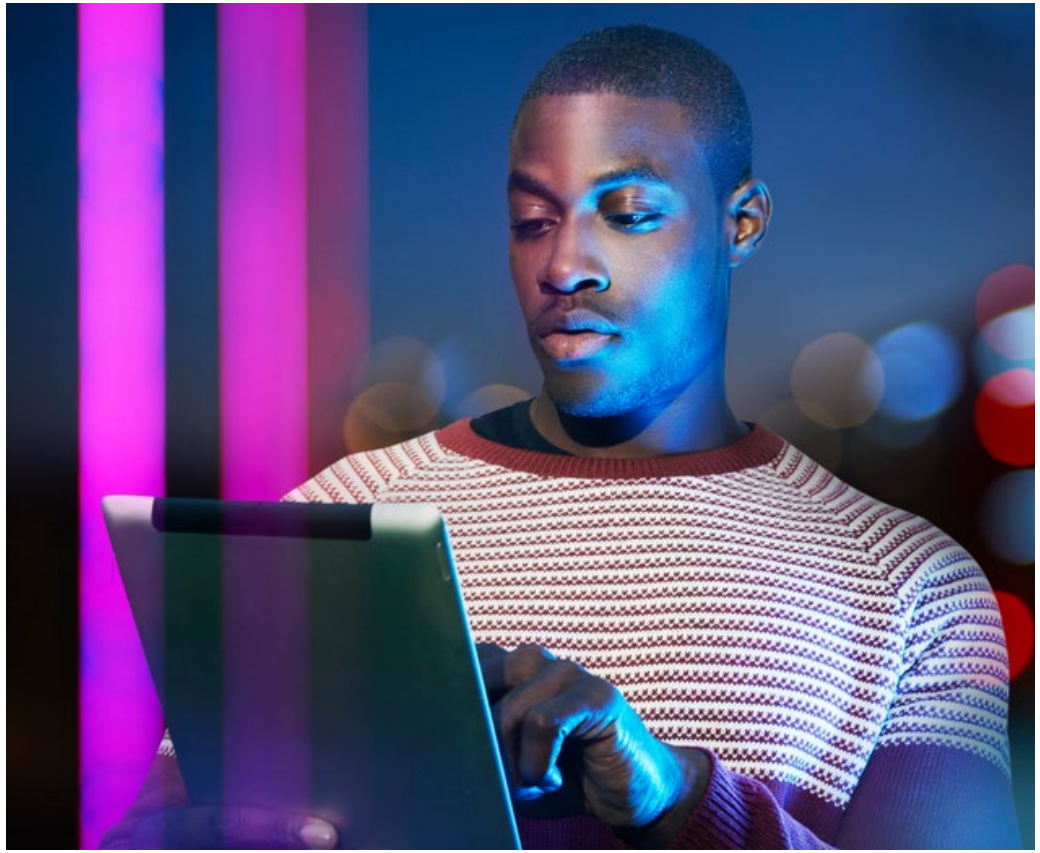
How Auditors Evaluate IPE

IPE Fundamentals for SOC Examinations

How Auditors Evaluate IPE

IPE vs. Audit Evidence

- Information Produced by the Entity (IPE) does **not** automatically qualify as audit evidence simply because it is system-generated or routinely used by management.
- Auditing standards require auditors to **evaluate the reliability** of all information used in testing, regardless of its source or format.
- Auditors assess **how the information is generated**, including the systems involved, report logic, parameters, and any manual intervention.
- Reliability depends on whether the information is **accurate**, meaning it correctly reflects underlying system activity and data.
- Auditors also evaluate **completeness**, ensuring that all relevant users, transactions, or events within scope are included in the population.
- Controls must exist to **prevent unauthorized changes** to report logic, underlying data, or report outputs after generation.



© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals for SOC Examinations

How Auditors Evaluate IPE

Why Reliability Determines Audit Conclusions

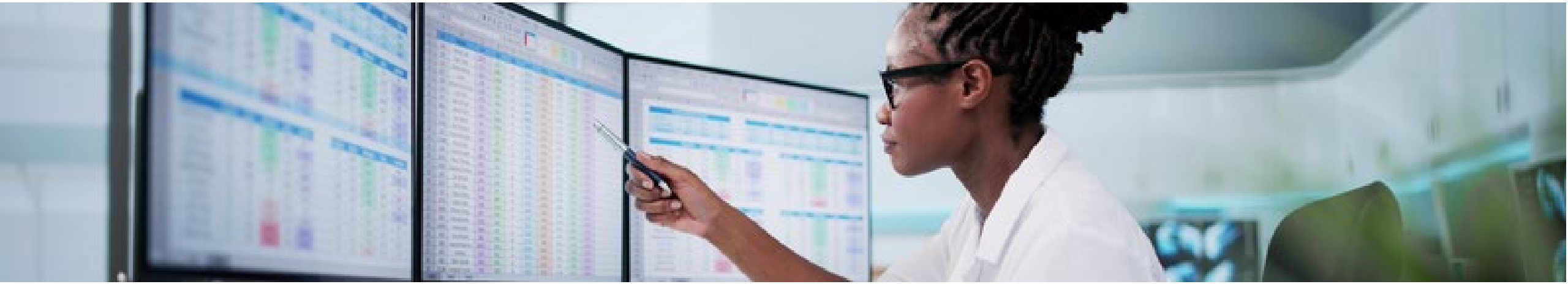
- When IPE is unreliable, auditors may be unable to place reliance on the evidence, even if the control itself appears properly designed and executed.
- Weaknesses in accuracy or completeness can result in expanded testing, additional evidence requests, or alternative audit procedures.
- In some cases, unreliable IPE may lead auditors to conclude that a control did not operate effectively, regardless of management's intent.
- Unreliable IPE often drives audit delays, re-work late in the examination period, and increased cost and effort for management.
- Repeated IPE issues can affect stakeholder confidence in the SOC report and complicate future examinations.

© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals for SOC Examinations

How Auditors Evaluate IPE

Management Responsibility for IPE



- Management is responsible for generating accurate and complete information.
- Service Auditors do not design reports or validate business logic; they assess whether controls over IPE are effective.
- IPE in SOC 1 and SOC 2 Examinations – SOC 1 focuses on financially relevant controls, while SOC 2 focuses on Trust Services Criteria. Despite these differences, auditor expectations for IPE reliability are consistent.
- Strong controls over report generation, review, and retention help ensure IPE can be relied upon and reduce downstream audit friction.

© 2026 Forvis Mazars, LLP. All rights reserved.

Common IPE Failures We See

Common IPE Failures We See

Incomplete Populations

Incomplete populations occur when reports do not fully capture all users, transactions, or activity within scope.

When populations are incomplete, auditors cannot conclude that the control addressed the full risk, regardless of how well the review was performed.

Even strong control design and execution may be overridden by unreliable population data.

Population issues often surface late in the audit, driving rework, delays, and increased cost.

© 2026 Forvis Mazars, LLP. All rights reserved.

Common IPE Failures We See

Unknown or Undocumented Report Logic

- If an organization cannot explain how a report is generated, auditors cannot rely on it.
- Documentation of logic and parameters is essential.

© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals for SOC Examinations
Common IPE Failures We See

Ownership & Accountability Gaps

Lack of clear ownership over reports often results in **unreliable IPE**, as no single individual is accountable for accuracy, completeness, or timeliness.

When ownership is unclear, report logic, parameters, and review processes are less likely to be **maintained or validated over time**, increasing audit risk.

Defining clear ownership establishes accountability for oversight, documentation, and issue resolution, leading to **more consistent evidence and improved audit outcomes**.

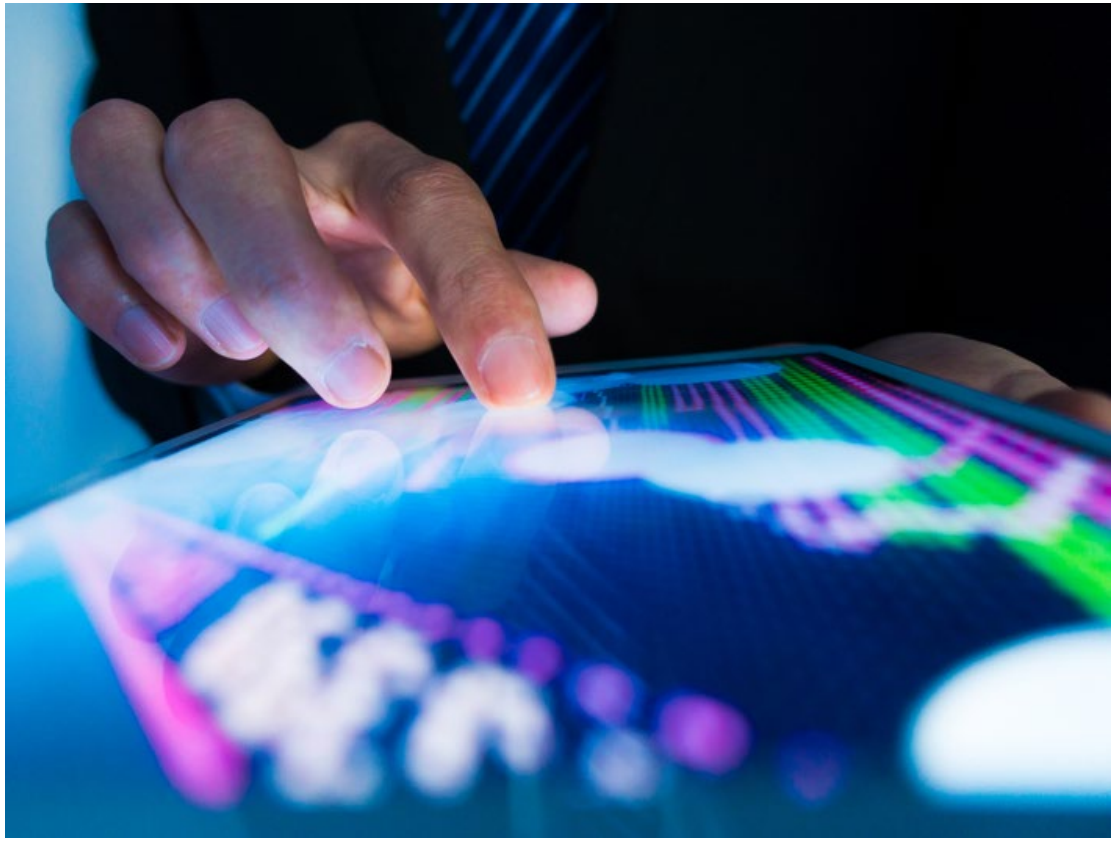
© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals for SOC Examinations

Common IPE Failures We See

Manual Manipulation of Reports

- Manual filtering or editing of reports introduces risk and often reduces auditor reliance compared to system-generated data
- Manual intervention increases the likelihood of unintentional error or data omission, particularly when performed outside of controlled processes.
- Without strong compensating controls, manually manipulated reports may not be accepted as reliable audit evidence, even when underlying data is accurate.



© 2026 Forvis Mazars, LLP. All rights reserved.

Strengthening IPE Reliability

IPE Fundamentals for SOC Examinations

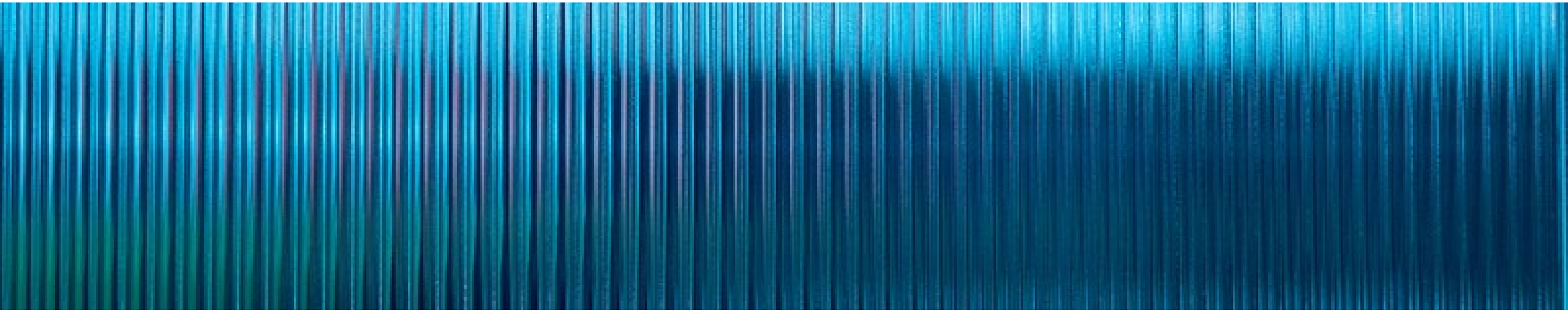
Strengthening IPE Reliability

Controls Supporting IPE Accuracy

- Accuracy is supported by **validating report logic**, including filters, calculations, and system queries used to generate the information.
- Reconciling report outputs to reliable source data helps confirm that information **accurately reflects** underlying system activity.
- Frequent review and testing of reports ensures accuracy is **maintained over time**, particularly after system or configuration changes.
- Reduction of “noise” in large data sets

© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals for SOC Examinations
Strengthening IPE Reliability



Controls Supporting IPE Completeness

Completeness is supported by **reconciling record counts** to expected totals to ensure no in-scope items are omitted.

Validating report **date ranges and parameters** helps confirm all relevant activity for the review period is captured.

Including all relevant account and transaction types—such as **privileged, service, and system accounts**—ensures the full population is assessed.

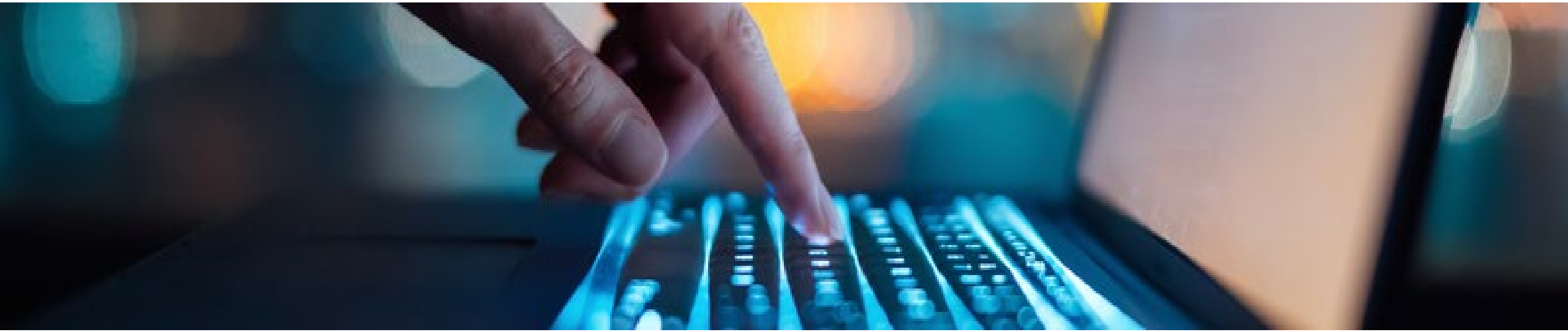
© 2026 Forvis Mazars, LLP. All rights reserved.

IPE Fundamentals for SOC Examinations

Strengthening IPE Reliability

Role of IT General Controls

- IT General Controls provide assurance that **report logic and underlying data cannot be altered** without authorization.
- Strong access and change management controls increase auditor confidence that IPE is **consistent, repeatable, and trustworthy**.
- Weak ITGCs often lead auditors to **increase testing or reduce reliance on IPE**, even when the report itself appears sound.



© 2026 Forvis Mazars, LLP. All rights reserved.

IPE in Practice

IPE Fundamentals for SOC Examinations

IPE in Practice

SOC 1 & SOC 2 IPE Examples

Common SOC 1 IPE

- User access listings are used to support controls over who has access to financially relevant systems and whether access is reviewed and approved appropriately.
- Change management reports support controls over changes to applications, configurations, or programs that could impact financial reporting.
- Processing and reconciliation reports are used to demonstrate the completeness and accuracy of transactions, interfaces, or batch processing activities.

Common SOC 2 IPE

- Logical access reports are used to demonstrate appropriate access to systems supporting the Trust Services Criteria.
- Change management reports support controls over system changes that could impact security, availability, or processing integrity.
- Monitoring outputs, such as alerts or logs, demonstrate ongoing oversight of system activity and potential security events.
- Incident logs are used to evidence detection, response, and resolution of security or operational incidents.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

IPE Fundamentals for SOC Examinations

IPE in Practice

Key Takeaways

- IPE is foundational to SOC examinations.
- Most issues stem from unreliable information rather than failed controls.
- Identify SOC-relevant IPE early, assign ownership, document logic, and proactively validate accuracy and completeness.
- Implement controls and systematic logging to reduce the risk of manual manipulation of IPE

© 2026 Forvis Mazars, LLP. All rights reserved.

Questions?

Contact

Forvis Mazars

Karen Cardillo
Managing Director
SOC & HITRUST Practice
karen.cardillo@us.forvismazars.com
704.452.8059

Ryan Boggs
Principal
SOC & HITRUST Practice
ryan.boggs@us.forvismazars.com
864.213.4034

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.