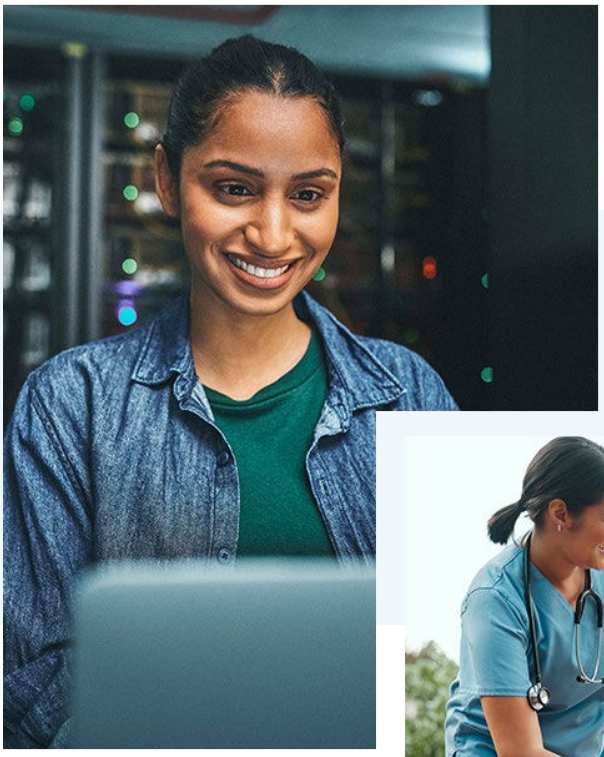
psi Testing Excellence



Case Study

How to use data forensics in the assessment lifecycle to increase test security

ISACA NAHQ National Association for Healthcare Quality

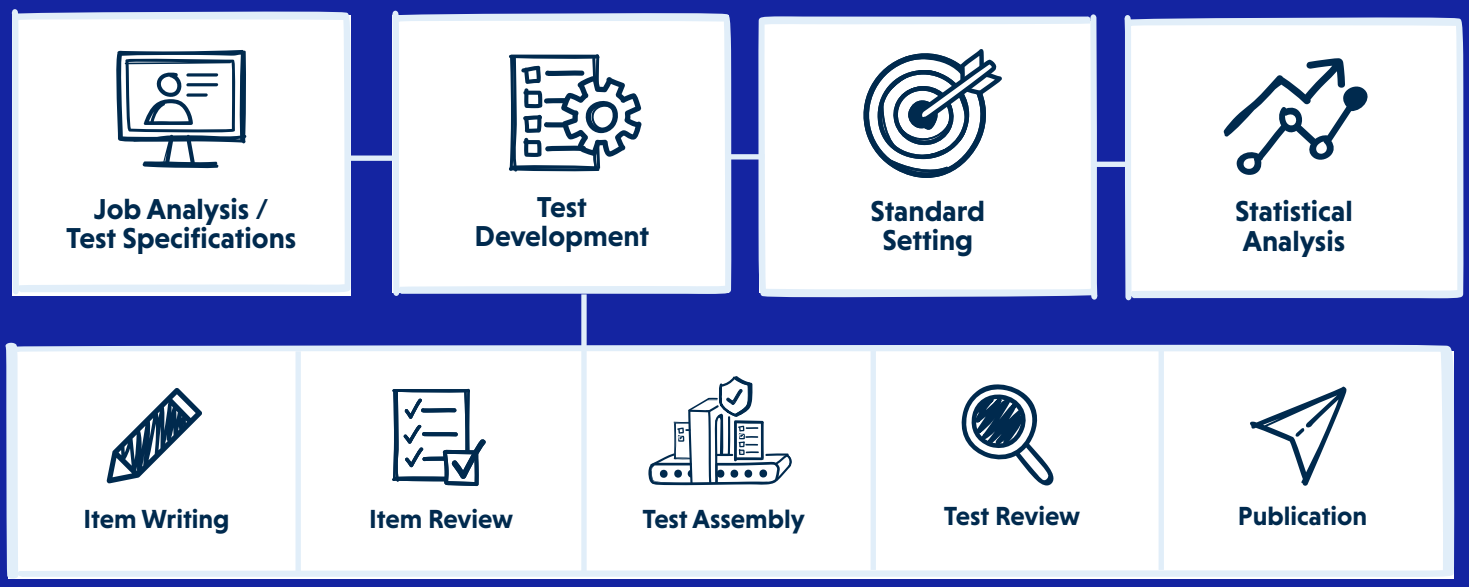
psiexams.com

Introduction

Bring data forensics into your assessment lifecycle to significantly enhance and improve test security.

Here's how your program can apply data forensics across different stages – from test development to test delivery and beyond.

Test development lifecycle

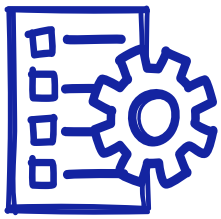


Job Analysis / Test Specifications

Define what needs to be assessed and how – your content outline or knowledge bank.

Test development

Content is developed to match what needs to be assessed.



Item writing

Test items written by Subject Matter Experts (SMEs) in the field.

Best practice example: A highly specialized topic limits the number of potential test items. When data forensics shows an item has been compromised or isn't properly testing the content, item writers are requested to write new items to replace compromised items.

Case study: ISACA uses data forensics to identify areas of need and support budget decisions about item development. When data analytics indicates items have been compromised, or over-exposed through frequent use, ISACA highlights these as priority areas for item writing. And where analytics shows an item is too easy, too difficult, or confusing, these items are prioritized for updating.

ISACA

Test assembly

Test forms are assembled to be equivalent and include a diversity of items and levels of difficulty. Using Linear on the Fly Test (LOFT) assembly helps limit the exposure of test items as test forms are different for each test taker.

Case study: In geographic regions where proxy testing and item harvesting are shown to be more prevalent, the National Association of Healthcare Quality (NAHQ) uses a smaller number of items in a test form than in other areas. When data analytics shows an increase in suspicious behaviors, forms are updated with new items.

NAHQ®
National Association for Healthcare Quality

Test review

Regular reviews of test items to ensure a test remains valid and current.

Case study: Where data analysis indicates that a topic or subtopic within the content outline has been compromised, this prompts targeted web crawling for that specific content. ISACA also uses data forensics to inform decision-making. For example, when web crawling locates stolen content on the internet or social media, data analysis is used to show the impact on test taker performance – and whether an item needs to be removed. This approach can be particularly helpful with specialized topics that have a small number of items.

ISACA

Standard setting

Setting a pass mark or grading that supports the mission of the organization and is consistent with the intended meaning of the credential.

"Our test security program exists to protect the public, the individuals we certify, and the reputation of our organization. That's why we do everything we can to protect the integrity of the exam and ensure anyone we certify meets the required level of competence in our exam content outline. Data forensics is particularly important as we expand internationally into areas where we don't understand the local norms."

Frank Perna
Director of Certification
NAHQ

Test delivery

Tests delivered securely to ensure fairness and an equitable experience regardless of modality.

Best practice example:

- Where an item has been exposed and shared with an incorrect answer, the item is used as a pre-test or unscored item to flag test takers using stolen test content.
- Analytics inform delivery policy for many testing organizations, for example when considering the adoption of online proctoring or multi-modal testing.
- Where a client looks after their own test admin, analytics supports test security by flagging potential issues at a particular test site or school.

ISACA

Case study: The PSI lockdown browser prevents the use of unauthorized applications – for example those that enable proxy testing or allow a test taker to access unsanctioned information during a test. ISACA uses the browser to not only detect but also prevent malpractice. Any applications opened during a test are recorded, not just those the team is currently aware of. When data analytics identifies a test taker as suspicious, any unusual applications that were open during their session are added to the list of unauthorized applications to prevent future use.

"Having PSI as a partner has been super, super helpful. It's one thing to have the numbers but being able to talk to people who understand them makes all the difference. It's only when you look at the data that you can see what is really happening."

Frank Perna
Director of Certification
NAHQ

Statistical analysis and reporting

Statistical trends and analytic techniques are employed to detect traces of fraudulent behavior that may indicate cheating.

Best practice example:

- **At a test taker level**, analysis shows similar responses across different test takers and unusual response times or patterns.
- **At an item level**, analytics reveals shifts in an item's average score.
- **At a group level**, analytics directs site auditors to regions or test sites with high rates of flagged test takers.
- **Further investigations** such as a review of test recordings or registration data. Plus secret shopper or drop-in inspections at a test site.

NAHQ®
National Association for Healthcare Quality

Case study: NAHQ uses PSI's data forensics reports to identify when unethical behavior or pre-knowledge may have occurred. The detailed reports include a deep dive into the data and what it means. Followed by recommendations for appropriate next steps from PSI psychometricians and security experts. Reports are discussed on regular calls where both teams agree how to proceed.

Putting data forensics into **action**

If further investigations find evidence of malpractice, PSI works with testing organizations to formulate an appropriate response.

Best practice example:

- Cease and desist letters to anyone sharing test content online, with enforced take down if necessary.
- Third-party test centers decommissioned or specific programs removed.
- Flagged test taker results reviewed before taking action.
- Review and update of testing policies to ensure test rules and the consequences of any breach are clear.

ISACA

Case study: The numbers tell a story. ISACA has a comprehensive Intellectual Property (IP) Infringement Policy. Where test content is found for sale online, their success rate for enforced take down averages 82% for web crawling campaigns. Data forensics has also prompted ISACA to review their eligibility requirements to increase test security even further.

"We can't have complete control at every stage of the assessment lifecycle. But we can control who we certify. It is hard to prove cheating, but data forensics enables us to identify individuals who have pre-knowledge and, in compliance with our candidate agreement, we enforce nullifications of their exam scores.

My advice to any organization considering a data forensics program with PSI is to do it. Work with your executive team to increase understanding and get buy-in from the start. Because without data forensics you run the risk of certifying individuals who do not meet your standards."

Kim Cohen
Senior Director – Credentialing,
ISACA

Connect with an expert today.

psiexams.com