PCI Security Standards Council®

Payment Card Industry (PCI)
Integrating Artificial Intelligence in PCI Assessments

Guidelines

Version 1.0

March 2025

Document Changes

Date	Version	Description
March 2025	1.0	Initial release.

© 2025 PCI Security Standards Council, LLC. All rights reserved.

Contents

© 2025 PCI Security Standards Council, LLC. All rights reserved.

1 Introduction

This document establishes guidelines for using AI in PCI assessments, including assessors' responsibilities in overseeing AI applications and procedures for ensuring that AI tools are implemented effectively and securely. It provides a framework for PCI qualified assessors to leverage the benefits of artificial intelligence (AI) to improve the speed and quality of their PCI assessments. This document also emphasizes the crucial role of human assessors in validating AI outputs and making final compliance decisions, highlighting that AI is a tool to aid—not replace—human expertise and judgment.

Integrating AI into assessments performed against the standards published and maintained by PCI SSC can assist with the efficiency, accuracy, and consistency of such assessments. AI technologies can automate and streamline various aspects of the assessment process, from document review to creating work papers and ROCs, thereby reducing manual effort and minimizing human error. However, AI systems and tools can also introduce false positives, incorrect assumptions, or biases, requiring additional considerations and stringent checks to prevent these issues. The assessor always remains responsible for all work performed.

Advancements in AI technologies have made technologies that use AI features broadly available. However, using AI in such critical assessments needs careful validation, oversight, and adherence to strict guidelines to ensure that data security as well as the integrity of the assessment is not compromised.

These guidelines provide a structure for incorporating AI into assessment processes and cover areas such as AI tool validation, managing AI biases, ensuring transparency in AI decision making, and integrating AI with existing assessment tools.

1.1 Purpose and Intended Use

This document describes how the use of artificial intelligence may be incorporated into practices for validating and assessing entities against the PCI standards.

These guidelines and procedures are intended to:

- Formalize an approach to support using AI in PCI assessments within defined parameters.
- Provide a consistent approach for assessors and assessor companies to follow.
- Incorporate industry best practices into uses of AI with PCI assessments.
- Maintain assessor responsibility for determining whether AI use is appropriate.

These guidelines DO NOT:

- Alter the applicability or the nature of assessment of any security requirements within a PCI standard.
- Provide an option to perform, or endorse the process of, a PCI assessment without the active involvement of an appropriately qualified and knowledgeable assessor.
- Imply that an AI system may be independently qualified to assess against any of the PCI standards.
- Aim to provide guidance or implementation advice for all scenarios where the use of AI may be used.

2 AI is a Tool, not an Assessor

AI cannot assume the role of an assessor. The lead assessor oversees the assessment process, making critical judgments, and ensuring the accuracy and completeness of the final report. AI can support tasks like data analysis and document review, in the same way a log management tool may help to filter out extraneous data from logs, but ultimate responsibility remains with the human assessor.

Examples of tasks AI should NOT perform include:

- Making final decisions or judgments regarding the compliance status of any individual requirement or final report.
- Interpretation of complex requirements or assessment of nuanced or context-specific issues.
- Authorizing release of assessment findings or final reports.
- Performing inspections or on-site evaluations.

Using AI in any part of an assessment must only be to support and enhance the work of human assessors, not replace them.

3 Transparent Client Communication

Where AI tools are used in the assessment process, assessors should ensure transparent and clear communication with clients. This includes informing clients of AI involvement, obtaining their consent, and providing assurances about the security of their data and the accuracy of assessment results.

3.1 Declaring AI Usage

A clear declaration of AI use should be provided to the assessed entity, and client consent should be obtained prior to using AI tools with customer data. This declaration should focus on:

- An overview of how AI will be used, and which tasks will be performed by AI.
- The role of AI in the assessment process.
- An overview of QA processes implemented to validate AI outputs and assurance that all AI outputs are reviewed and approved by human assessor.
- Information about data handling and security practices specific to AI processes.
- Information about training data, models used, description of data transfers, and ongoing maintenance of the AI tool.

Clients should also be kept informed of any significant changes in how AI is used during their assessment. By clearly communicating AI usage and maintaining transparency, assessors can build client trust while responsibly using AI to enhance the quality and efficiency of PCI assessments.

4 AI Use in PCI Assessments

4.1 Review of Artifacts

AI can automate the review of large volumes of documents during assessments, including policies, procedures, network diagrams, software source code, system configurations, and logs. During automated reviews, AI can identify specific compliance elements such as consistency of content, revision dates, and the presence or absence of required items, highlighting potential areas of concern.

For instance, some AI systems can quickly parse through thousands of logs to identify compliance issues that might take a human assessor days to uncover. While AI handles large datasets and complex documents quickly, it is critical to validate AI technologies for accuracy and reliability. Assessors are responsible for continuously reviewing AI performance to ensure alignment with expected results. This includes ongoing training and updates to AI algorithms to enhance accuracy and reliability, ensuring that AI systems remain compliant with applicable PCI requirements.

Human oversight and quality assurance (QA) processes are essential for verifying AI findings and ensuring outputs meet expectations. These processes also help confirm that the AI system continues to perform reliably over time.

When an entity under assessment uses its own AI tools to monitor and maintain PCI compliance, assessors cannot rely on the AI's assessment of evidence. While an AI tool can evaluate a wide range of systems and data, assessors are required to perform independent sampling, examinations, and interviews in accordance with PCI testing requirements. Ultimately, the assessor's judgment is necessary to confirm whether compliance requirements have been met. Key Points

- AI can automate the review of large volumes of documents.
- AI tools may be able to analyze text data for specified content and context.
- Assessor companies should have validation procedures that include benchmarking AI performance and regular updates to AI algorithms.
- Assessors are required to employ human oversight and QA processes to verify AI findings.

4.2 Creation of Work Papers

AI can assist with the creation of work papers by organizing data, providing preliminary analysis and summaries, and suggesting areas for further investigation. This use of AI can reduce manual effort and human error. For example, AI can automatically generate summaries based on data inputs and flag areas that need further human investigation.

Whenever AI is used to create work papers, assessors are expected to use a suitably qualified person or persons to validate all outputs for accuracy and completeness. For example, an AI model being used to generate network diagrams should have its accuracy and completeness verified by a network engineer. Assessors are expected to confirm that all outputs meet the requirements of the relevant standard, and to review content before any work papers are completed. Adopting a dual approach that includes AI and human review helps maintain the high standards required for assessor documentation.

Key Points

- AI organizes data and provides preliminary analysis.

- Work papers must be accurate, consistent, and complete.
- Human assessors are expected to review and validate AI outputs as part of a comprehensive QA process.

4.3 Conducting Remote Interviews

AI can be used to facilitate remote interviews by scheduling, transcribing conversations, and summarizing key points. For example, AI tools can automatically transcribe interviews and highlight the relevant requirements in a standard that may need to be reviewed later in the assessment. In all cases, the tools used should comply with data privacy, contractual requirements, and security regulations, as required. Additionally, assessors should record AI usage and validate transcriptions and summaries for accuracy with all parties involved. Adopting these steps ensures transparency for all parties while maintaining the integrity of the interview process.

Key Points

- AI can schedule and transcribe interviews.
- AI tools should comply with data privacy, such as interviewee consent, and security regulations.

5 AI Use in Creating Suggested Wording for Final Assessment Reports

5.1 Final Assessment Reports

AI can be used to assist with the creation of final assessment reports. For example, AI tools can suggest phrasing, summarize findings, or structure content according to PCI SSC reporting templates. AI tools can also analyze the assessment data and suggest specific wording for sections such as executive summaries, compliance status, and recommendations based on reporting templates and industry best practices. AI can also summarize detailed findings into concise, understandable language, making the reports more accessible to various stakeholders.

However, the use of AI in report generation requires careful oversight. Accordingly, the lead assessor reviews and approves AI-generated content, incorporating QA reviews to ensure it accurately reflects assessment results and is in line with the testing procedures of the relevant standard, including any criteria in the related Program Guide and Qualification Requirements. This involves thorough validation, where assessors compare AI-generated content with the findings and ensure that all critical details and nuances are captured accurately.

Key Points

- AI can suggest phrasing and summarize findings.
- Lead assessor reviews and approves AI-generated content.
- Lead assessor confirms that content aligns with the testing procedures and program requirements of the relevant standard(s).

5.2 Addressing AI Challenges

Given the complexity of AI models, transparency and traceability in how AI processes data and generates outputs is critical. AI systems should provide traceable decision-making paths for review during the assessor's internal AI QA processes, mitigating the risk of accepting AI outputs without a clear understanding of the rationale behind them. Additionally, the assessor's AI QA processes should include regular bias checks of the output as part of the validation to ensure fairness and accuracy in AI-generated findings. Importantly, the validation of AI output accuracy should be conducted independently, with a qualified individual who did not code or develop the tool itself.

The assessors' AI QA processes, focused on validating AI system outputs, should not be confused with the assessors' reporting QA processes, which ensure final report accuracy and compliance.

5.3 Validation Process

The assessor company should include the following in their validation processes for any final assessment report:

- Cross-referencing AI-generated content with raw assessment data.
- Ensuring AI suggestions align with, and utilize where necessary, any templates for the standards under assessment.
- Verifying the accuracy and completeness of summaries and suggested phrasings.

- Regularly updating AI tools to reflect changes in the related standards and other relevant guidelines.

In addition to validating AI-generated outputs, it is essential for assessor companies to implement robust QA processes specific to AI. This includes cross-verifying AI results with manual assessments to ensure consistency, accuracy, and completeness. QA checks should be an integral part of the assessment process, helping to detect any discrepancies or errors introduced by AI.

5.4 Keep AI Policies and Procedures Current

As the use of AI continues to develop, the need to keep AI assessment policies and procedures becomes increasingly important. These policies and procedures should provide detailed guidance on AI tool selection, usage, and QA processes. The aim is to ensure that any new AI tools or processes are integrated responsibly and effectively, while ensuring all applicable security and compliance requirements are maintained. Continuous improvement of AI tools and processes is essential.

5.5 Limitations and Risks

While AI can enhance efficiency and quality, it can also make mistakes. AI might misunderstand complex findings, generate incorrect content, or produce generic content that does not fully capture assessment specifics. For example, AI models might misinterpret requirement nuances in security settings or produce summaries that overlook key assessment factors. Assessors should be aware of these limitations and be prepared to adjust AI-generated content accordingly.

5.6 Integration with Templates

AI tools should be integrated with existing PCI SSC reporting templates to ensure consistency and alignment. Assessor company QA processes must include confirmation that AI outputs match specific format and content requirements, ensuring that final documents remain consistent within the industry.

5.7 Ethical and Legal Considerations

When using AI to generate report content, or review artifacts during an assessment, it is essential to maintain the confidentiality of assessment data. AI tools should be designed to avoid biases and ensure that all content is generated ethically and transparently. Assessors and assessor companies should document processes for AI usage and ensure compliance with relevant legal and regulatory requirements.

6 Responsibility and Accountability

The lead assessor and the assessment company are responsible for assessment outcomes, including overseeing AI use throughout the assessment process and ensuring AI-generated outputs meet the subject PCI standard, and committing to continuous improvement of AI tools and processes. This includes regularly evaluating AI systems for accuracy, reliability, and alignment with PCI SSC requirements, and updating algorithms to address any biases or errors identified over time. If quality issues are found in output generated by an AI system, any impacts of that can be expected to be imposed on the lead assessor and assessor company. AI may be used as a tool, but as a tool it cannot be held responsible. The responsibility, accountability, and quality of PCI SSC assessments ultimately rest with the assessor and assessor company, as outlined in the respective PCI SSC program guides.

Key Points

- Lead assessors and assessor companies take ultimate responsibility.
- Oversee AI use and ensure standards are met.
- Continuously improve AI tools and processes.

7 Documented Policies and Procedures for AI Use

To ensure the effective and secure integration of AI in PCI assessments, it is crucial for each assessor company to establish clear and detailed policies and procedures for AI use. These procedures help maintain the integrity, accuracy, and security of the assessment process. Documented procedures provide a standardized approach for assessors, ensuring that AI tools are configured, validated, and used consistently across all assessments.

As AI continues to evolve, there is a need for ongoing development of comprehensive AI assessment policies. These policies should provide detailed guidance on AI tool selection, usage, and QA, facilitating secure and accurate integration of AI into assessments.

The following items should be documented by assessor companies using AI:

7.1 How AI is to be Used and Validated

- Outline specific tasks for AI, such as analyzing logs or summarizing findings.
- Provide detailed steps for configuring AI tools to align with assessment requirements.
- Include initial testing against known benchmarks, validation of output and the model, and updating AI models to reflect changes in assessment criteria.
- Ensure human oversight for all AI-generated outputs through rigorous QA processes to validate accuracy, consistency, and alignment with PCI standards.

7.2 Selection and Qualification of AI Systems

- Define criteria for selecting AI systems, including accuracy, reliability, security features, and compliance with regulatory requirements.
- Establish a qualification process involving rigorous testing and validation.
- Ensure that training data originates from authorized, anonymized sources and that AI tools do not inadvertently use sensitive client or third-party data for training purposes.

7.3 Types of Evidence AI Can Process

- Define the evidence AI can process, such as text documents, configuration files, logs, and digital communications.
- Use AI only for evidence types for which it has been tested and approved by the assessor company.
- Limit AI functions to assessment-related tasks, ensuring no unintended data processing occurs.

7.4 Data Handling and Security

- Establish protocols for data handling, including acquisition, processing, secure storage, and deletion.
- Ensure compliance with security measures, data retention, and privacy policies and any applicable legislation.
- Evidence sharing in PCI assessments should be strictly for confirming compliance or conformance and not for ancillary activities, such as training AI systems or large language models (LLMs).

- Contractual agreements should clearly state the use of sensitive data, such as configurations, network diagrams, or compliance findings, in AI training datasets is forbidden.
- Clients should be informed about how their data will be handled, particularly in relation to AI usage, and assurances provided that their information will not contribute to internal or external training datasets unless explicitly authorized.

8 PCI SSC Non-Endorsement of AI Products or Services

The PCI Security Standards Council (PCI SSC) does not endorse, recommend, or qualify any specific products or services for PCI assessments. Assessment companies and individual assessors are expected to evaluate and select AI tools based on their criteria and due diligence.

As such, assessment companies and individual assessors should:

- Conduct thorough evaluations of AI tools before use.
- Establish criteria for evaluating AI tools, including accuracy, reliability, security, and compliance with the requirements in relevant PCI standards.
- Implement a pilot phase to thoroughly test all AI tools before full deployment.

By maintaining clear guidelines and procedures, assessment companies and individual assessors can ensure AI tools are used responsibly and effectively, enhancing the efficiency and accuracy of PCI assessments while upholding the highest standards of security and compliance.

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. Our role is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders. To learn more, please visit pcisecuritystandards.org.