Experian EI3PA Frequently Asked Questions

(Technical Providers/Agents of End Users/Platform Providers)

What is EI3PA?

- Experian's Independent 3rd Party Assessment (EI3PA) is an annual assessment of a Third Party's ability to protect Experian provided data.
- Experian and its Third Parties face significant risks if the consumer information we provide is not adequately protected. Experian would violate its principles of exercising due care and due diligence by selling its products and services to customers who cannot protect them at least as well as Experian does. Protecting the consumer data entrusted to both Experian and its clients is the right thing to do.

What does EI3PA require?

- EI3PA requires an evaluation of a Third Party's information security program and controls by an independent assessor, based on requirements provided by Experian.
- EI3PA consists of security controls requirements adapted from PCI-DSS.
- Additionally, the following are EI3PA unique requirements that must also be met:
    - External vulnerabilities scans - to be submitted to EI3PA on a quarterly basis
    - Multi-Factor Authentication - for commercial users/non-direct to consumer access to web portals

Is this assessment the same as PCI-DSS?

- No, EI3PA differs from PCI-DSS in that it assesses how a Third Party provides protection of Experian-provided data rather than cardholder data.
- It also differs in that it is approved solely by Experian, not by the card issuer, issuing bank or the assessor.

How often does the assessment need to be performed?

- EI3PA is an annual assessment and certification. It must be renewed within one-year from the date of current certification.

Who must perform the assessment?

- Experian's policy is that the same vendors who perform assessments for PCI compliance are qualified to perform assessments for EI3PA.
- The assessment must therefore be performed by a PCI Qualified Security Assessor (QSA) as defined and listed by the PCI-SSC on their website. https://www.pcisecuritystandards.org/qsa_asv/find_one.shtml

Are there other certifications or assessments we can submit to meet EI3PA requirements?

- The following standard certifications can be leveraged to meet EI3PA requirements:
    - ISO 27001
    - PCI-DSS (Level 1)
    - SOC2 Type II
    - FISMA
    - CAI/CCM Assessment
- For those certifications to be considered, Experian EI3PA team will need to review the assessment report and obtain attestation from the assessor for the following:
    - The scope of the review included all systems that receive, store, process, or deliver Experian data.
    - EI3PA certification requirements have been received, understood, and agreed to be met on annual basis. Attestation of requirements being met, include, but not limited to:
        - Experian's Multi-Factor Authentication (MFA) requirements are met.
        - External vulnerability scan is performed on a quarterly basis and performed by PCI Approved Scanning Vendor (ASV).

What form does the EI3PA assessment report take?

- The expected deliverable at the end of the EI3PA assessment is a report on compliance, documented in the Experian Security Assessment Report (ESAR Level 1) workbook by the independent assessor.
- Reports on compliance and all results of EI3PA assessments as well as any other related artifacts are maintained as Confidential under Experian's Information Security Policy.

Who receives the report?

- The electronic report and artifacts should be sent to the EI3PA mailbox (EI3PA@Experian.com)

The report is confidential to our company. Who at Experian will have access to it?

- Access to the report is restricted to the Experian Global Security Office (GSO) team that reviews it.

Will we be able to claim 'EI3PA Level 1 Certified' status when the assessment is finished?

- Yes, once the submitted report has been reviewed and confirmed to meet Experian requirements.
- A certification letter will be provided in writing by Experian and will outline the effective dates.
- Any publication of 'EI3PA Level 1 Certified' status must follow Experian branding guidelines.
- Please contact the EI3PA team at EI3PA@Experian.com for further information regarding branding and disclosure.

Who must perform the quarterly external vulnerability scans?

- The same vendors who perform scans for PCI compliance are qualified to perform scans for EI3PA.
- The vendors are referred to as PCI ASV as defined and listed on the PCI-SSC website, and sent to Experian. In many cases, this may be the same vendor as your QSA. https://www.pcisecuritystandards.org/pdfs/asv_report.html.

What must be included in the quarterly external vulnerability scans?

- Experian provided data environment must be included in the scope of the external vulnerability scan, not cardholder data.

How much will an EI3PA assessment cost?

- The assessed entity is responsible for securing the assessment engagement with the QSA.
- The cost is entirely dependent upon the contract negotiated with the QSA.

Can Experian help us negotiate with the QSA?

- No, this could impair the independence of the QSA and the objectivity of Experian.

What assistance is available from Experian?

- Experian is available to confer with the QSA to answer questions about EI3PA requirements and assure the QSA understands the elements to be assessed.

What are Experian's requirements when using IaaS (Infrastructure as a Service) or PaaS (Platform as a Service) cloud providers such as Amazon AWS?

- EI3PA security requirements are shared between the Third Party and the cloud provider.
- Cloud or hosted service providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
    - ISO 27001
    - PCI-DSS (Level 1)
    - EI3PA
    - SOC2 Type II
    - FISMA
    - CAI/CCM Assessment

Where can I get more information?

- Experian's Third Party Technical Providers page at http://www.experian.com/corporate/vendors.html
- The EI3PA mailbox at EI3PA@Experian.com