**What is the Security Technology Enhancement Program (STEP)?**
The Security Technology Enhancement Program (STEP) is a way that American Express recognizes the investments Merchants make in improving the security of Cardholder data. Merchants that qualify for STEP are no longer required to submit quarterly vulnerability scan results.

**Do I qualify for STEP?**
To qualify for the Security Technology Enhancement Program (STEP) there are several qualifications to which you must attest:

- No Data Incidents in the previous 12 months
- Current compliance with the Payment Card Industry Data Security Standard (PCI DSS)
- Must meet all the annual vulnerability scan requirements

To qualify for Security Technology Enhancement Program (STEP) there are several qualifications to which you must attest.

**What is the Security Technology Enhancement Program or STEP?**
The Security Technology Enhancement Program (STEP) reduces the number and complexity of annual validation requirements for American Express Merchants. Merchants that qualify for STEP:

- Do not have to conduct any quarterly vulnerability scan requirements.
- Will not be required to submit any other annual PCI document (ROC or SAQ) or a quarterly vulnerability scan results.

**What is the Security Technology Compliance Program?**
The Security Technology Compliance Program (STEP) is a way that American Express recognizes the investments Merchants make in improving the security of Cardholder data. Merchants that qualify for STEP are no longer required to submit quarterly vulnerability scan results.

**How can I find additional information about STEP?**
Log back into TrustKeeper® PCI Manager. Upload your completed annual STEP Attestation form.

**What are the benefits of qualifying for STEP?**
Merchants that qualify for STEP:

- Only submit an annual STEP Attestation form as their annual PCI validation requirement.
- If you previously qualified as an American Express Level EMV Merchant, you may submit the Annual EMV Attestation (AEA) and submit only an annual STEP Attestation form as their annual PCI validation requirement.
- Voluntary participation in the Security Technology Compliance Program (STEP) makes it easier for Merchants to validate their PCI compliance, which is a requirement by all U.S. card payment environments.

**What is PCI DSS?**
The Payment Card Industry Data Security Standard (PCI DSS) has been developed to protect Cardholder data. Merchants must ensure that all Cardholder data is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach.

**What is EMV?**
EMV means an integrated circuit card (sometimes called an “IC Card,” “chip card,” or “smart card”). Under EMV a Merchant has an accounting system that allows for the secure processing of transactions. Merchants must be enrolled in a PCI-approved EMV solution.

**What if American Express requires different PCI validation documentation with the physical Card present?**
If you are still required to submit an annual Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) to another card brand, the American Express PCI Compliance Program will also accept those same documents.

**What if American Express requires different PCI validation documentation with the physical Card present and originate from EMV Chip-Enabled Devices?**
If you are still required to submit an annual Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) to another card brand, the American Express PCI Compliance Program will also accept those same documents.

**How does STEP compare with other validation relief programs?**
Other card brands also offer PCI validation reduction/relief programs. However, the American Express Security Technology Compliance Program makes it easier for Merchants to validate their PCI compliance, which is a requirement by all U.S. card payment environments.

**How do I submit my application for STEP today?**
If you are already enrolled in the STEP Attestation from the Payment Card Industry Security Standards Council website (www.pcisecuritystandards.org), you have an account established with the Trustwave secure portal. To log in, see the instructions on thePortal Login page.

**What is QSA?**
A Qualified Security Assessor (QSA) who has been trained by Payment Card Industry Security Standards Council (PCI SSC). In this case, a Qualified Security Assessor (QSA) has also been trained by Payment Card Industry Security Standards Council (PCI SSC). A QSA has been trained to test and validate the functionality of the Point-to-Point Encryption solution in the Merchant’s environment. The QSA’s report is submitted to the PCI Data Security Standards Council (PCI SSC) on behalf of the Merchant.

**What is PCI Approved P2PE?**
The Payment Card Industry Security Standards Council (PCI DSS) has established a list of companies that have successfully completed a validation testing. The list of compliant solutions is updated on the PCI Web site so Merchants are not required to submit quarterly vulnerability scans.

**What is QSA Approved P2PE?**
Some companies have an effective Point-to-Point Encryption solution that has not yet been approved by PCI SSC. In this case, a Qualified Security Assessor (QSA) has also been trained by Payment Card Industry Security Standards Council (PCI SSC). Through EMV-compliant terminals, OR:

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Required documentation</th>
<th>American Express</th>
<th>Yes</th>
<th>N/A</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 (&gt;2.5 million)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Level 2 (50k to 2.5 million)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Level 3 (&lt;50k &gt;10K)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Level 4 (&lt;10K)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**How do I submit my application for STEP today?**

**What is the Security Technology Compliance Program?**
The Security Technology Compliance Program (STEP) is a way that American Express recognizes the investments Merchants make in improving the security of Cardholder data. Merchants that qualify for STEP are no longer required to submit quarterly vulnerability scan results.

**What is PCI Approved P2PE?**
The Payment Card Industry Security Standards Council (PCI DSS) has established a list of companies that have successfully completed a validation testing. The list of compliant solutions is updated on the PCI Web site so Merchants are not required to submit quarterly vulnerability scans.

**What is QSA Approved P2PE?**
Some companies have an effective Point-to-Point Encryption solution that has not yet been approved by PCI SSC. In this case, a Qualified Security Assessor (QSA) has also been trained by Payment Card Industry Security Standards Council (PCI SSC). Through EMV-compliant terminals, OR:

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Required documentation</th>
<th>American Express</th>
<th>Yes</th>
<th>N/A</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 (&gt;2.5 million)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Level 2 (50k to 2.5 million)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Level 3 (&lt;50k &gt;10K)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Level 4 (&lt;10K)</td>
<td>Submit the SAQ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**How do I submit my application for STEP today?**

**What is the Security Technology Compliance Program?**
The Security Technology Compliance Program (STEP) is a way that American Express recognizes the investments Merchants make in improving the security of Cardholder data. Merchants that qualify for STEP are no longer required to submit quarterly vulnerability scan results.

**What are the benefits of qualifying for STEP?**
Merchants that qualify for STEP:

- Only submit an annual STEP Attestation form as their annual PCI validation requirement.
- If you previously qualified as an American Express Level EMV Merchant, you may submit the Annual EMV Attestation (AEA) and submit only an annual STEP Attestation form as their annual PCI validation requirement.
- Voluntary participation in the Security Technology Compliance Program makes it easier for Merchants to validate their PCI compliance, which is a requirement by all U.S. card payment environments.

**What is PCI DSS?**
The Payment Card Industry Data Security Standard (PCI DSS) has been developed to protect Cardholder data. Merchants must ensure that all Cardholder data is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach.

**What is EMV?**
EMV means an integrated circuit card (sometimes called an “IC Card,” “chip card,” or “smart card”). Under EMV a Merchant has an accounting system that allows for the secure processing of transactions. Merchants must be enrolled in a PCI-approved EMV solution.

**What if American Express requires different PCI validation documentation with the physical Card present?**
If you are still required to submit an annual Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) to another card brand, the American Express PCI Compliance Program will also accept those same documents.

**What if American Express requires different PCI validation documentation with the physical Card present and originate from EMV Chip-Enabled Devices?**
If you are still required to submit an annual Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) to another card brand, the American Express PCI Compliance Program will also accept those same documents.

**How does STEP compare with other validation relief programs?**
Other card brands also offer PCI validation reduction/relief programs. However, the American Express Security Technology Compliance Program makes it easier for Merchants to validate their PCI compliance, which is a requirement by all U.S. card payment environments.

**How do I submit my application for STEP today?**

**What is the Security Technology Compliance Program?**
The Security Technology Compliance Program (STEP) is a way that American Express recognizes the investments Merchants make in improving the security of Cardholder data. Merchants that qualify for STEP are no longer required to submit quarterly vulnerability scan results.

**What are the benefits of qualifying for STEP?**
Merchants that qualify for STEP:

- Only submit an annual STEP Attestation form as their annual PCI validation requirement.
- If you previously qualified as an American Express Level EMV Merchant, you may submit the Annual EMV Attestation (AEA) and submit only an annual STEP Attestation form as their annual PCI validation requirement.
- Voluntary participation in the Security Technology Compliance Program makes it easier for Merchants to validate their PCI compliance, which is a requirement by all U.S. card payment environments.

**What is PCI DSS?**
The Payment Card Industry Data Security Standard (PCI DSS) has been developed to protect Cardholder data. Merchants must ensure that all Cardholder data is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach.

**What is EMV?**
EMV means an integrated circuit card (sometimes called an “IC Card,” “chip card,” or “smart card”). Under EMV a Merchant has an accounting system that allows for the secure processing of transactions. Merchants must be enrolled in a PCI-approved EMV solution.