



Visa U.S.A. Cardholder Information Security Program (CISP)
Frequently Asked Questions

Contents

CISP Program Overview 2

1. To whom does CISP apply? 2
2. What does VISA define as "cardholder data"? 2
3. What if a merchant or service provider does not store Visa cardholder data? 2
4. When is it acceptable to store magnetic stripe data? 2
5. When is it acceptable to store Card Verification Value 2 (CVV2)? 2
6. Are there alternatives, or compensating controls, that can be used to meet a requirement? 2
7. Are there alternatives to encrypting stored data? 3
8. What if a Member, merchant, or service provider has outsourced the storage, processing, or transmission of cardholder data to a service provider? 3
9. Other than the Visa Web site, where can I direct any questions about CISP? 3
10. Can a merchant/service provider be considered CISP compliant if they have outstanding non-compliance issues, but provide a remediation plan? 3

Impact of Industry Alignment on CISP 4

11. When must merchants and service providers begin using the new Payment Card Industry materials? 4
12. What is the impact of the PCI data security standards to merchants and service providers who have already implemented the CISP requirements? 4

Compliance Validation – Merchants and Service Providers 5

13. If a merchant or service provider has already validated compliance with CISP, do they need to re-validate using the PCI Data Security Standard? 5
14. Where can a list of security assessors qualified to complete the Report On Compliance and/or scan vendors qualified to complete the Network Security Scan be found? 5
15. Where can the Self-Assessment Questionnaire be found? 5
16. What is a Network Security Scan? 5
17. Is the Network Security Scan only applicable to e-commerce entities? 5
18. Is it a common practice for security assessors to perform a re-assessment? 6
19. How do merchants and service providers determine the cost of compliance validation? 6

Compliance Validation – Merchants Only 6

20. Have the compliance validation requirements changed for Level 1 Merchants as a result of the alignment? 6
21. Have the compliance validation requirements changed for retailers who were formerly Level 2 Merchants, but now are considered Level 4? 6
22. What are the compliance validation reporting requirements for merchants? 6
23. How is the transaction volume that determines a merchant’s compliance level measured? 6
24. What is the scope of the onsite review for Level 1 Merchants? 7
 - o How is “IP-based POS environment” defined? 7
25. Do merchants need to include their service providers in the scope of their CISP review? 7

Compliance Validation – Service Providers Only 8

26. Have the compliance validation requirements changed for service providers? 8
27. Are the compliance validation requirements for service providers aligned? 8
28. What are the compliance validation reporting requirements for service providers? 8
29. How is the transaction volume that determines a service provider’s compliance level measured? 8
30. What is the scope of the onsite review for Level 1 and 2 Service Providers? 8

Frequently Asked Questions

CISP Program Overview

1. To whom does CISP apply?

CISP is directed to all entities that store, process, or transmit Visa cardholder data.

2. What does VISA define as "cardholder data"?

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. The account number is the critical component that makes CISP applicable. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data, however, CISP applies even if the only data stored, processed, or transmitted is account numbers.

3. What if a merchant or service provider does not store Visa cardholder data?

If a merchant or service provider does not store cardholder data, CISP still applies to the environment that transmits or processes cardholder data.

4. When is it acceptable to store magnetic stripe data?

It is never acceptable for Acquirers, merchants, or service providers to retain magnetic stripe data subsequent to transaction authorization. The Visa Operating Regulations prohibit storage of the contents of the magnetic stripe as a unit. The following individual data elements may be retained subsequent to transaction authorization:

- Cardholder Account Number
- Cardholder Name
- Card Expiration Date

5. When is it acceptable to store Card Verification Value 2 (CVV2)?

It is never acceptable for Acquirers, merchants, or service providers to retain CVV2, which consists of the last three digits printed on the signature panel of all Visa Cards, subsequent to transaction authorization. The Visa Operating Regulations prohibit such storage, whether encrypted or unencrypted.

6. Are there alternatives, or compensating controls, that can be used to meet a requirement?

If a requirement is not, or cannot, be met exactly as stated, compensating controls can be considered as alternatives to requirements defined in CISP. Compensating controls should meet the intention and rigor of the original CISP requirement, and should also be examined by the assessor as part of the regular CISP audit. Compensating controls should be "above and beyond" other CISP requirements - it is not a compensating control to simply be in compliance with other CISP requirements.

Frequently Asked Questions

7. Are there alternatives to encrypting stored data?

Stored cardholder data should be rendered unreadable according to requirement 3 of the PCI Security Audit Procedures document. If encryption, truncation, or another comparable approach cannot be used, encryption options should continue to be investigated as the technology is rapidly evolving. In the interim, while encryption solutions are being investigated, stored data must be strongly protected by compensating controls. These compensating controls should be considered as part of the compliance validation process.

An example of compensating controls for encryption of stored data is complex network segmentation that may include the following:

- Internal firewalls that specifically protect the database
- TCP wrappers or firewall on the database to specifically limit who can connect to the database
- Separation of the corporate internal network on a different network segment from production, fire-walled away from database servers.

8. What if a Member, merchant, or service provider has outsourced the storage, processing, or transmission of cardholder data to a service provider?

Members, merchants, and service providers should be in the process of positioning themselves to deal only with CISP-compliant service providers. If there are service providers handling cardholder data on an entity's behalf, the entity must ensure that contracts with these service providers specifically include CISP compliance as a condition of business. A list of compliant service providers can be found on the [CISP Website](#).

9. Other than the Visa Web site, where can I direct any questions about CISP?

You may direct questions regarding CISP by e-mailing AskVisaUSA@visa.com.

10. Can a merchant/service provider be considered CISP compliant if they have outstanding non-compliance issues, but provide a remediation plan?

Lack of full compliance will prevent an entity from being considered CISP compliant, however, Visa encourages entities to complete the initial review, develop a remediation plan, complete items on the remediation plan, and revalidate compliance of those outstanding items. For service providers, a Report On Compliance demonstrating full compliance must be provided to Visa prior to inclusion on the list of compliant service providers. Currently, there is not a comparable list for merchants.

Impact of Industry Alignment on CISP

11. When must merchants and service providers begin using the new Payment Card Industry materials?

The Payment Card Industry Standards, Security Audit Procedures, Self-Assessment Questionnaire, and Security Scanning Requirements are effective immediately. For compliance validation assessments beginning before 2005, merchants and service providers may continue to use the last version of the CISP materials. For compliance validation assessments not yet underway, the updated Payment Card Industry materials should be used going forward to ensure acceptance by other card brands.

12. What is the impact of the PCI data security standards to merchants and service providers who have already implemented the CISP requirements?

Realizing that many Members, merchants, and service providers have already gone to great lengths to ensure their CISP compliance, Visa has mapped the PCI Data Security Standards to the last version of the CISP requirements published in the Visa U.S.A. Security Audit Procedures and Reporting document. This mapping document can be located on the Visa CISP web site as www.visa.com/cisp.

Members, merchants, and service providers will find that each of the former "Digital Dozen" and their associated sub-requirements remain intact within the PCI Data Security Standard. It was necessary for Visa to make some changes to CISP to develop an mutually acceptable payment card industry standard, however, as the CISP requirements have proven effective in combating data security threats, the majority of the requirements remain substantially unchanged.

Frequently Asked Questions

Compliance Validation – Merchants and Service Providers

13. If a merchant or service provider has already validated compliance with CISP, do they need to re-validate using the PCI Data Security Standard?

Visa appreciates the efforts of merchants and service providers operating within the compliance requirements of CISP, and their efforts to fulfill their compliance validation obligations for previous years. Visa will continue to recognize these efforts until the entity reaches their revalidation due date. As CISP requires ongoing compliance validation, Member, merchants, and service providers who have already validated compliance with CISP must consider the PCI Data Security Standard and the aligned compliance validation requirements as they prepare for revalidation due dates.

14. Where can a list of security assessors qualified to complete the Report On Compliance and/or scan vendors qualified to complete the Network Security Scan be found?

A list of Visa-approved security assessors can be found on the [CISP Website](#).

15. Where can the Self-Assessment Questionnaire be found?

The *Self-Assessment Questionnaire* is available on the [CISP Website](#). Many of the qualified Scan Vendors offer merchants and service providers the option to complete the *Compliance Questionnaire* on the security assessor's Web site. Alternatively, merchants and service providers may download and complete the soft copy available on the CISP Web site.

16. What is a Network Security Scan?

A Network Security Scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. As provided by qualified scan vendors, the tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

17. Is the Network Security Scan only applicable to e-commerce entities?

No. The System Perimeter Scan is applicable to all merchants and service providers with external-facing IP addresses. Even if an entity does not offer Web-based transactions, there are other services that make systems Internet accessible. Basic functions such as e-mail and employee Internet access will result in the Internet-accessibility of a company's network. These seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems if not properly controlled. If a merchant or service provider does not have any external-facing IP addresses they will only be required to complete the *Report On Compliance* or the *Compliance Questionnaire*, as appropriate.

Frequently Asked Questions

18. Is it a common practice for security assessors to perform a re-assessment?

Yes, we ask the assessor to re-validate those items that were not in place at the time of the initial review and provide an updated Report on Compliance.

19. How do merchants and service providers determine the cost of compliance validation?

The cost of the onsite review, for Level 1 Merchants and service providers, varies greatly depending on the size of the environment to be reviewed, the chosen assessor, and the degree to which the entity is already in compliance when the review commences. The cost of a Network Security Scan depends on the number of IP addresses to be scanned, the frequency of the scans, and the chosen scan vendor. Merchants and service providers should contact the qualified security assessors, found on the [CISP Website](#), for more specific pricing information.

Compliance Validation – Merchants Only

20. Have the compliance validation requirements changed for Level 1 Merchants as a result of the alignment?

Level 1 Merchants will find the compliance validation requirements virtually unchanged; however, they must use the aligned PCI materials, including the Security Audit Procedures and Security Scanning Procedures, when they revalidate compliance during their next annual review. The alignment will not impact the schedule of a Level 1 Merchant's next annual revalidation due date.

21. Have the compliance validation requirements changed for retailers who were formerly Level 2 Merchants, but now are considered Level 4?

Some card-present merchants formerly at CISP Level 2 have been placed in the new compliance Level 4 category. For these merchants, CISP validation requirements are now optional. This does not, however, alleviate their obligation to ensure compliance with CISP. As such, Visa strongly encourages merchants in this category to validate compliance via completion of the annual self-assessment questionnaire and network scan.

22. What are the compliance validation reporting requirements for merchants?

The CISP and SDP compliance validation requirements for merchants have also been aligned so that merchants need only validate their compliance once to fulfill their obligation to all payment cards accepted. Merchants will provide compliance validation documentation to their Acquirer(s). Though the compliance validation process is aligned for merchants, Acquirers must follow each payment card company's respective reporting requirements to ensure that a merchant's status is appropriately filed with each.

23. How is the transaction volume that determines a merchant's compliance level measured?

The number of transactions will be determined based on the gross number of Visa transactions processed by a DBA or a chain of stores—not of a corporation that owns several chains. Acquirers are responsible for identifying the appropriate compliance validation levels of their merchants. For

Frequently Asked Questions

Level 2 and 3 Merchants, only e-commerce transaction volume is used to determine a merchant's compliance validation level. For all levels, if a merchant meets the compliance validation criteria based on Visa OR MasterCard transaction volume, they must comply with the requirements of that compliance validation level. If a merchant falls into one level based on Visa transaction volume and another based on MasterCard transaction volume, they must comply with the more stringent validation requirements.

24. What is the scope of the onsite review for Level 1 Merchants?

Members are responsible for the security of Visa cardholder data wherever it is resident and any liability that may occur as a result of non-compliance with CISP; however, the scope of CISP compliance validation for Level 1 Merchants is focused on any system(s) or system component(s) related to authorization and settlement where Visa cardholder data is retained, stored, or transmitted, including:

- All external connections into the merchant network (i.e.; employee remote access, VisaNet, third party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (i.e.; connections for employee access or for devices such as firewalls, and routers)
- Any data repository outside of the authorization and settlement environment where more than 500 thousand account numbers are stored.
- POS Terminals may be excluded, however:
 - If a POS environment is IP-based and there is external access, via Internet, wireless, VPN, dial-in, broadband, or publicly accessible machines (such as kiosks), to the merchant location, the POS environment must be included in the scope of the on-site review.
 - If a POS environment is either not IP-based or there is no external access to the merchant location, begin review at the connection into the authorization and settlement environment.
 - ***How is "IP-based POS environment" defined?***
The POS environment is the environment in which a transaction takes place at a merchant location (i.e. retail store, restaurant, hotel property, gas station, supermarket, or other point-of-sale location). An IP-based POS environment is one in which transactions are stored, processed, or transmitted on IP-based systems, or systems communicating via TCP/IP.

25. Do merchants need to include their service providers in the scope of their CISP review?

No. Service providers are responsible for validating their own compliance with CISP independent of their customers. Acquirers must identify service providers handling cardholder data on their merchant's behalf. Visa will then work with Acquirers to ensure that these service providers validate compliance with CISP.

Compliance Validation – Service Providers Only

26. Have the compliance validation requirements changed for service providers?

Service providers will find the CISP compliance validation process and selection criteria virtually unchanged; however, when they revalidate their compliance during their next annual review, they must use the PCI materials, including the Security Audit Procedures and Security Scanning Procedures. The alignment will not impact the schedule of a service provider's next annual revalidation due date.

27. Are the compliance validation requirements for service providers aligned?

There may be differences in compliance validation requirements for service providers across the payment card companies. Service providers may be categorized differently by each payment card brand; however, the compliance validation methodologies are aligned between Visa and MasterCard. This includes the Security Audit Procedures document used to perform the onsite review, the Security Scanning Procedures, and the Self-Assessment Questionnaire.

28. What are the compliance validation reporting requirements for service providers?

Visa requires service providers to provide the compliance validation documentation directly to Visa. Once compliance has been validated, Visa will include compliant service providers on the List of Compliant Service Providers on the [CISP Website](#).

As there may be differences in the compliance validation requirements for service providers across the payment card companies, service providers should confirm the acceptability of these results to fulfill the compliance validation requirements of other payment card companies. Service providers may be required to submit compliance validation documentation to other payment card companies or financial institutions.

29. How is the transaction volume that determines a service provider's compliance level measured?

For Level 2 and 3 Service Providers the number of accounts/transactions will be determined based on the gross number of Visa transactions or accounts stored, processed, or transmitted—not just for the merchant or Member supported but for all entities supported by a service provider. Transaction volume is not considered for Level 1 Service Providers as all VisaNet Processors and payment gateways fall into Level 1.

30. What is the scope of the onsite review for Level 1 and 2 Service Providers?

CISP compliance validation for Level 1 Service Providers must be performed on any system(s) or system component(s) involved in storing, processing, or transmitting Visa cardholder data.