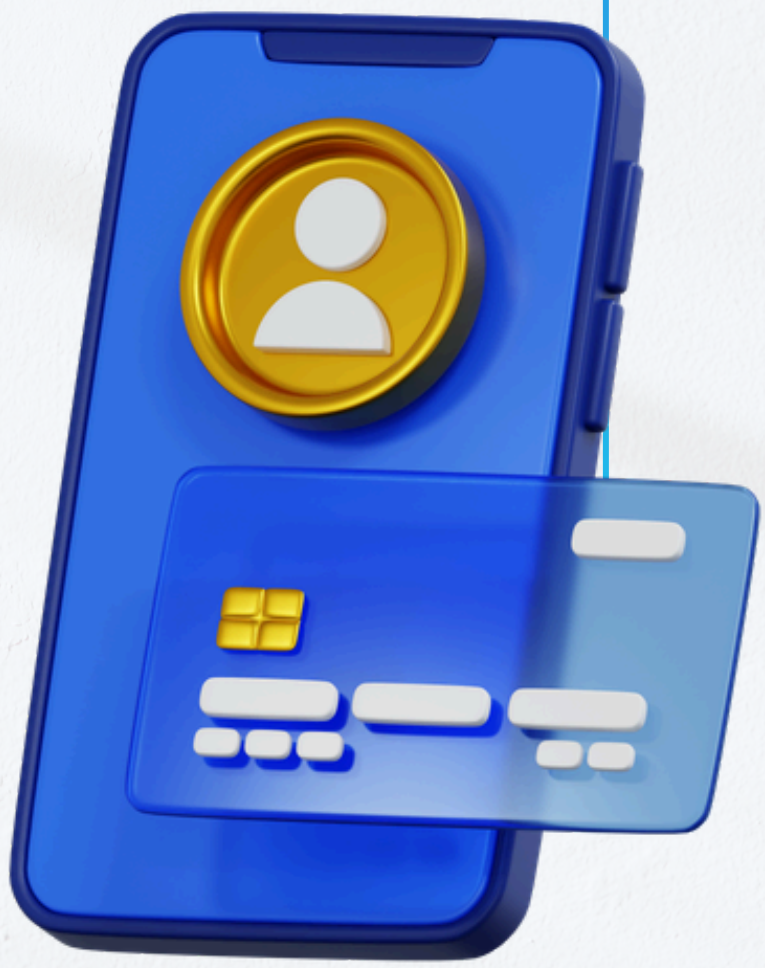
SECUREB4
We Strengthen Your Security

4

PCI DSS

Compliance Levels

Explained



Secureb4.global

SECUREB4
We Strengthen Your Security

What Are the PCI DSS Compliance Levels?

Adherence to the PCI DSS is mandatory for all merchants and service providers that store, process, or transmit credit card information. info@secureb4.global

The primary function of the PCI DSS is to decrease instances of credit card fraud and to enhance data protection measures.

The importance of PCI compliance lies not only in preserving a company's integrity but also in safeguarding consumer data by preventing security vulnerabilities and data breaches.

PCI Level 1

Applies to large-scale merchants processing in excess of 6 million transactions annually.

PCI Level 2

Applies to large merchants processing between 1 million and 6 million transactions annually.

PCI Level 3

Relevant to mid-sized merchants with an annual transaction volume ranging from 20,000 to 1 million.

PCI Level 4

Specific to small merchants processing fewer than 20,000 transactions annually.

info@secureb4.global

SECUREB4
We Strengthen Your Security

PCI Level 1 Compliance

PCI Level 1 encompasses organizations that process above 6 million credit card transactions annually, including the majority of large-scale international retailers. The requirements specific to Level 1 entities are as follows

- **External Audits:** Level 1 organizations are mandated to commission third-party audits conducted by a PCI-approved Qualified Security Assessor (QSA). These audits evaluate the company's physical security measures and digital data protection protocols to confirm PCI-DSS compliance.

- **Compliance Report:** Upon conclusion of the audit, companies receive a Report on Compliance (ROC) that provides recommendations for areas requiring improvement and outlines the steps necessary for complete PCI-DSS compliance.

- **Compliance Attestation:** Level 1 entities must complete an Attestation of Compliance (AOC) and submit it to the PCI-DSS SSC. This document elaborates on the organization's compliance strategy, supplements the ROC, and may detail specific security issues more comprehensively.

- **Periodic Network Scans:** Level 1 organizations are required to perform quarterly network scans, executed by an Approved Scanning Vendor (ASV). These scans identify potential vulnerabilities, and it is incumbent upon the client to heed their recommendations and rectify any detected faults.

- **Penetration Testing:** Annual penetration testing is also advised for these organizations, to ensure robust security measures.

SECUREB4
We Strengthen Your Security

PCI Level 2 Compliance

Level 2 entities, those handling between one to six million cardholder transactions annually, have a distinct set of security protocols to ensure PCI compliance, albeit less rigorous than Level 1.

Self-Assessment Questionnaire (SAQ)

Level 2 entities are not normally subject to external audits. Instead, they are required to submit a comprehensive Self-Assessment Questionnaire (SAQ) to the PCI-DSS Security Council. Varying SAQ templates are accessible on the PCI SSC website, tailored to the unique compliance requisites of each organization.

Situation-Specific Audits

In certain instances, Level 2 merchants may necessitate an external audit, predominantly in the aftermath of a data breach or any cybersecurity incident within the preceding year.

PCI Compliance Reports

Level 2 entities are mandated to deliver a Report of Compliance (ROC) form. This document can be internally generated, with external consultation typically unnecessary.

Demonstration of PCI-DSS Compliance

Each Level 2 merchant is obligated to demonstrate their PCI-DSS compliance. Regular penetration and network tests conducted by approved vendors are a requisite. The ROC must furnish evidence of rigorous data security protocols.

SECUREB4
We Strengthen Your Security

PCI Level 3 Compliance

The PCI-DSS Level 3 designation identifies merchants who annually manage between 20,000 and 1 million transactions. This classification shares similar requirements with Level 2, with one notable exception: JCB International (formerly Japan Credit Bureau) does not differentiate between Levels 2 and 3, instead grouping all entities exceeding 20,000 transactions under Level 2. For those adhering to the more common standard, Level 3 merchant obligations include:

- **Completion of Self-Assessment Questionnaires (SAQs):** These are essential to demonstrate unambiguous adherence to applicable PCI-DSS norms.

- **Implementation of PCI-DSS Compliant Controls and Routine Testing:** Merchants are expected to engage approved vendors to execute quarterly network scans, acting promptly to rectify any exposed security vulnerabilities. Although it is considered good security protocol, penetration testing does not constitute a requirement for Level 3 merchants.

SECUREB4
We Strengthen Your Security

PCI Level 4 Compliance

Designated as Level 4 by PCI-DSS standards, merchants conducting fewer than 20,000 transactions annually fall within this tier. It's critical to note that VISA classifies any merchant handling up to 1 million transactions per year also as a Level 4 entity. The compliance requirements for Level 4 merchants are less stringent. They are exempt from obligatory external audits, penetration testing, or the submission of a Report on Compliance (ROC). However, their responsibilities encompass:

Execution of Quarterly Network Scans

An Approved Scanning Vendor (ASV) must be appointed by Level 4 merchants to conduct network scans on a quarterly basis.

Completion of Self-Assessment Questionnaires

All Level 4 entities are required to fill out a self-assessment compliance form.

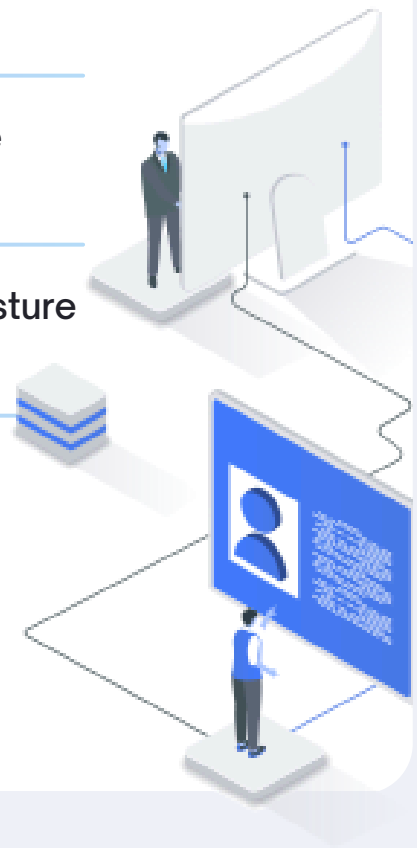
Submission of an Attestation of Compliance

The Attestation of Compliance (AOC) is a document that offers the PCI-DSS council insights into the merchant's compliance strategy and any historical data breaches, if applicable.

Our Service Offerings

SECUREB4
We Strengthen Your Security

- Vulnerabilities Management and Compliance (VM)
- Vulnerabilities Discloser Program (VDP)
- Passwordless Authentication
- Privacy and Consent Management
- Privileged Access Manager (PAM)
- Patch Management
- Open-Source Software Protection
- Integrated Digital Risk Protection (IDRP)
- Identity and Access Management (IDAM)
- Cloud Security Posture Management (CSPM)
- Behaviors based Multifactor authentications
- Age Assurance and Online Safety (AAAOS)
- Continuous Threat Exposure Management (CTEM)
- Cyber Risk and Compliance (Secure Operator)
- Attack Surface Management (ASM)
- Breach and Attack Simulation (BAS)
- Bug Bounty Program (BBP)
- Cloud Security and Compliance
- Continuous Automated Red teaming (CART)
- Data Foresight and VM Foresight
- External Threat Landscape Management (ETLM)
- End-to-End Encryption and Data Protection
- Extend Security Posture Management (XSPM)
- Application Security Posture Management (ASPM)
- Data Security Posture Management (DSPM)



www.secureb4.global
info@secureb4.global

SECUREB4
We Strengthen Your Security

Get In Touch With Us.

Have Questions?
We're Just a Message Away!

Our Phone:

+971 565612349

Our Website:

www.secureb4.global

Our Email:

info@secureb4.global