SnowBe Online PCI DSS Audit

Merchant Level, SAQ Scope & Compliance Assessment

A collaborative PCI DSS assessment determining SnowBe Online's merchant level, applicable Self-Assessment Questionnaire, cardholder-data-environment scope, and ongoing compliance obligations.

PCI DSS | SAQ D | Cardholder Data Environment | ASV Scanning | Compliance | Cloud Security

AT A GLANCE

Scenario	SnowBe Online: ~1.2 million card transactions a year (90% of sales), cardholder data stored in an AWS-hosted WordPress storefront
Determinations	PCI DSS Level 2 merchant · SAQ D v3 Merchant · annual SAQ and AOC · quarterly ASV scans
Scope	AWS environment, WordPress shopping cart, databases, servers, endpoints, VPN and network devices unless segmented and verified out of scope

Sean Richard

sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. Substantive project content is preserved; classroom-only submission headers were removed.

MERCHANT LEVEL

Level 2

1M–6M transactions / year

APPLICABLE SAQ

SAQ D

v3 Merchant — stores cardholder data

VALIDATION

SAQ + AOC

Annual, plus quarterly ASV scans

01 — MERCHANT LEVEL

Which PCI merchant level applies to SnowBe Online, and why

SnowBe Online is a PCI DSS Level 2 merchant. The case study states that credit and debit card purchases account for 90 percent of sales and equal approximately 1,200,000 transactions per year. PCI Merchant Level 2 generally applies to merchants that process between 1 million and 6 million payment card transactions annually. SnowBe does not meet the Level 1 threshold of more than 6 million annual transactions, but it exceeds the transaction limits for Levels 3 and 4. Therefore, based on the transaction volume provided in the case study, Level 2 is the correct merchant level.

This matters because the merchant level determines the PCI DSS validation and compliance requirements SnowBe must meet. SnowBe processes a high volume of card transactions and stores credit card information through its website. Since PCI DSS applies to organizations that store, process, or transmit cardholder data, SnowBe's AWS environment, WordPress shopping cart, databases, servers, access management systems, network devices, and connected systems are considered part of the PCI DSS environment unless properly segmented and verified out of scope.

02 — REQUIREMENTS

What is required under Level 2

As a PCI DSS Level 2 merchant, SnowBe Online is required to complete several compliance and security requirements to help protect customer payment information. Since the company processes about 1.2 million payment card transactions every year, it falls into the Level 2 category. Under this level, SnowBe is required to complete an annual Self-Assessment Questionnaire (SAQ), an Attestation of Compliance (AOC), and quarterly vulnerability scans performed by an Approved Scanning Vendor (ASV). The SAQ helps evaluate whether the company is following PCI DSS security requirements, while the AOC confirms the company completed the assessment and understands its responsibilities. Quarterly ASV scans are required to identify vulnerabilities that could place cardholder data at risk.

SnowBe must also maintain security controls across systems that store, process, or transmit cardholder data. This includes the company's AWS environment, WordPress shopping cart, databases, servers, employee laptops, office desktops, VPN connections, and network devices. PCI DSS requires organizations to maintain firewalls, regularly update systems, use antivirus software, secure passwords, restrict access to sensitive information, and monitor systems for suspicious activity. Because SnowBe stores customer payment information on its systems, the company has a larger PCI DSS scope and greater responsibility to properly secure cardholder data. Although improvements

were made, such as updating antivirus software and patching systems, the case study still shows concerns involving access control and shared login information. Because of this, SnowBe would still need continuous monitoring, documentation, testing, and ongoing security improvements to remain compliant with PCI DSS Level 2 requirements.

03 — SAQ SELECTION

Which SAQ applies, and why the others do not

SAQ D v3 Merchant is the appropriate SAQ for SnowBe Online because the company stores and processes payment card information through its website hosted on AWS. The case study explains that most sales are completed through SnowBe's website and that credit cards are accepted and stored there. Customer information and purchase history are also stored indefinitely. Since SnowBe stores and processes cardholder data electronically through its website, the company has a larger PCI DSS scope than businesses that fully outsource payment processing.

SAQ	WHY IT DOES NOT FIT SNOWBE
SAQ A	SnowBe has not fully outsourced payment processing.
SAQ A-EP	SnowBe's website and WordPress shopping cart are directly involved in the payment process.
SAQ B, B-IP, C-VT, P2PE	Do not apply because of how SnowBe handles payment processing and cardholder data.
SAQ C	Intended for merchants with internet-connected payment applications that do not electronically store cardholder data; SnowBe does store it.
SAQ D v3 Merchant	**Selected.** Covers SnowBe's broader cardholder data environment: website, WordPress cart, stored cardholder data and connected systems.

Based on the case study, there is no requirement to complete multiple SAQs. The physical storefronts use bank-provided terminals that are PCI DSS Level 1 certified and do not store customer information. The case assumptions state that payments not processed through the website are cash or check. Although AWS is PCI DSS Level 1 certified as a service provider, SnowBe remains responsible for securing its website, WordPress shopping cart, stored cardholder data, and connected systems. For these reasons, SAQ D v3 Merchant is the best and most complete SAQ for SnowBe Online because it covers the company's broader cardholder data environment.

04 — ONGOING OBLIGATIONS

What else SAQ D requires

Since SnowBe Online falls under SAQ D v3 Merchant, there are additional responsibilities beyond simply completing the questionnaire. Because SAQ D applies to organizations with a broader PCI DSS scope, SnowBe would need to complete regular security testing, maintain documentation, and continue implementing strong security controls for systems that store, process, or transmit cardholder data.

This includes regular vulnerability scans, system updates, access control reviews, strong password protections, monitoring systems for suspicious activity, and employee security awareness training. SnowBe would also need to maintain records showing that security controls are being followed and continue making improvements if weaknesses are identified. In addition, SnowBe would be expected to maintain an Attestation of Compliance (AOC), complete quarterly ASV scans, and continuously validate PCI DSS controls due to the large scope of systems involved. Since the case study shows concerns such as shared login information and access control issues, SnowBe would need regular monitoring and continuous security improvements to remain compliant with PCI DSS requirements.