1. *What PCI merchant level applies to SnowBe Online? Why? Be thorough in your explanation.*

Merchant Level 2 applies to SnowBe because they have transactions of over 1,200,000 every year from credit and debit cards. Merchant Level 2 is a specific category that is issued to businesses that process transactions of one to six million annually. Handling sensitive cardholder data on their Wordpress shopping cart and AWS-hosted environment elevates the company's risk profile, making level 2 compliance mandatory.

2. *What must SnowBe do under this level? Be thorough in your response.*

SnowBe is required to conduct assessments once a year using self-assessment questionnaires and may need a quarterly PCI ASV scan. Level 2 merchants will not require on-site PCI DSS audits unless they have been breached or a cyberattack has occurred. This is all a part of the compliance required to continue business.

3. *Which SAQ(s) applies to SnowBe Online? Why? Be thorough in your explanation. If SnowBe Online is required to complete more than one SAQ, be sure to list and explain why for each. Be thorough in your explanation.*

SAQ D Merchant and Service Provider is one SAQ that applies to SnowBe. It is essentially the basic SAQ that goes towards any business that is a service provider and stores cardholder data. These are both true for SnowBe as cardholder data is held inside their servers and they provide financial services for their customers. SAQ P2PE also fits with SnowBe's circumstance as it is a SAQ meant for merchants using hardware payment terminals. SnowBe has ATMs and stores that allow customers to pay or acquire bank information.

4. *What else, if anything, is required based on the SAQ requirement? IF nothing, be sure to state that. Be thorough in your explanation.*

Enhance Access Controls: Enforce individual user IDs and strong password policies, while also implementing role-based access control to limit access to cardholder data

Inspect Payment Terminals: Regularly inspect physical payment terminals for tampering or unauthorized modifications.

Conduct Vulnerability Scanning and Monitoring: Perform internal and external vulnerability scans regularly and maintain logs for all systems accessing sensitive data.

5. *Statement of agreement for the SAQ group portion. "I (fill in your name) agree with the information that is in our group SAQ and agree to accept the grade that our group receives."*

I Michael Kohronas agree with the information that is in our group SAQ and agree to accept the grade that our group receives.

References

https://pcidssguide.com/choosing-the-right-pci-dss-saq/

https://pcidssguide.com/pci-dss-compliance-levels/