Below is a list of the 22 questions included in **SAQ A** for PCI DSS compliance. These questions are grouped under the applicable PCI DSS requirements for SAQ A, which are **Requirements 2, 8, 9, and 12**. I've summarized each question to help you understand what's being asked.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

1. **Changing Default Passwords and Settings**
    - **Question**: Have you changed all vendor-supplied default passwords and security settings on your systems before installing them on your network?
    - **Explanation**: Default passwords are well-known and can be easily exploited. Ensure all defaults are replaced with strong, unique passwords.
2. **Removing Unnecessary Default Accounts**
    - **Question**: Have you removed or disabled any unnecessary default accounts before installing systems on your network?
    - **Explanation**: Unused default accounts can be entry points for attackers. Disable or remove any that aren't needed.

Requirement 8: Identify and Authenticate Access to System Components

3. **Assigning Unique User IDs**
    - **Question**: Do you assign a unique ID to each person with access to cardholder data or systems?
    - **Explanation**: Unique IDs ensure accountability and traceability of actions taken on systems.
4. **Implementing Strong Authentication Methods**
    - **Question**: Do you employ strong authentication methods (like strong passwords) for all users?
    - **Explanation**: Strong authentication reduces the risk of unauthorized access.
5. **Password Policies and Management**
    - **Question**: Do you have password policies requiring minimum length, complexity, and regular changes?
    - **Explanation**: Robust password policies enhance security by making passwords harder to guess or crack.
6. **Secure Password Storage and Transmission**
    - **Question**: Are passwords securely stored and transmitted (e.g., encrypted)?
    - **Explanation**: Protects passwords from being intercepted or accessed in plaintext.
7. **User Account Management Procedures**
    - **Question**: Do you have procedures for adding, deleting, and modifying user accounts and access?

- **Explanation**: Proper account management ensures that only authorized users have access.

8. **Removing Inactive User Accounts**
    - **Question**: Are inactive user accounts removed or disabled within 90 days?
    - **Explanation**: Reduces the risk of old accounts being exploited.
9. **Physical Access Control for Authentication Devices**
    - **Question**: Do you ensure that devices used for authentication (like tokens or smart cards) are assigned to individuals and not shared?
    - **Explanation**: Prevents unauthorized use of authentication devices.

Requirement 9: Restrict Physical Access to Cardholder Data

10. **Physical Access Controls to Systems**
    - **Question**: Do you use physical security controls to restrict access to systems that store, process, or transmit cardholder data?
    - **Explanation**: Physical barriers prevent unauthorized personnel from accessing sensitive areas.
11. **Visitor Identification and Logging**
    - **Question**: Do you properly identify and authorize visitors, and maintain a log of visitor activity to sensitive areas?
    - **Explanation**: Keeps track of who is entering sensitive areas and when.
12. **Securing Media Containing Cardholder Data**
    - **Question**: Do you securely store media containing cardholder data in locked areas?
    - **Explanation**: Protects physical media (like USB drives, CDs) from unauthorized access.
13. **Destruction of Media When No Longer Needed**
    - **Question**: Do you destroy media containing cardholder data when it's no longer needed, so data cannot be reconstructed?
    - **Explanation**: Prevents recovery of sensitive data from discarded media.
14. **Logging and Management Approval for Media Movements**
    - **Question**: Do you maintain strict control over the internal or external distribution of any kind of media that contains cardholder data?
    - **Explanation**: Ensures all movements of sensitive media are tracked and approved.

Requirement 12: Maintain a Policy That Addresses Information Security

15. **Information Security Policy Documentation**
    - **Question**: Do you have a documented information security policy that is reviewed at least annually and communicated to all personnel?
    - **Explanation**: A formal policy sets the organization's security expectations and responsibilities.

16. **Daily Operational Security Procedures**
    - **Question**: Do you have daily operational security procedures consistent with PCI DSS requirements?
    - **Explanation**: Ensures ongoing compliance and security in daily activities.
17. **Security Awareness Program for Personnel**
    - **Question**: Do you have a security awareness program to educate personnel on the importance of cardholder data security?
    - **Explanation**: Training helps employees understand their role in protecting data.
18. **Incident Response Plan Documentation**
    - **Question**: Do you have an incident response plan to respond to system breaches or data theft?
    - **Explanation**: Preparedness to handle security incidents minimizes damage and recovery time.
19. **Service Provider List Maintenance**
    - **Question**: Do you maintain a list of service providers who handle cardholder data, including a description of services provided?
    - **Explanation**: Knowing who your service providers are is essential for managing compliance.
20. **Service Provider PCI DSS Compliance Monitoring**
    - **Question**: Do you monitor your service providers’ PCI DSS compliance status at least annually?
    - **Explanation**: Ensures that third parties maintain required security standards.
21. **Written Agreements with Service Providers**
    - **Question**: Do you have written agreements with service providers acknowledging their responsibility for cardholder data security?
    - **Explanation**: Formal agreements hold service providers accountable.
22. **Annual Incident Response Plan Testing and Personnel Training**
    - **Question**: Do you test your incident response plan at least annually and train relevant personnel on their responsibilities?
    - **Explanation**: Regular testing and training ensure the plan is effective and everyone knows their role.

These 22 questions are designed to confirm that you, as a merchant eligible for SAQ A, have appropriate policies and procedures in place to protect cardholder data, even though you outsource all cardholder data functions to third-party service providers. They focus on ensuring that your organization:

- Does not store, process, or transmit cardholder data on your own systems or premises.
- Has proper security policies and procedures.
- Manages and monitors service providers' compliance.
- Maintains physical security controls where applicable.
- Ensures personnel are aware of security responsibilities.

Note: While these questions are summaries, it's crucial to refer to the official SAQ A document provided by the PCI Security Standards Council for the exact wording and to ensure full compliance. Consulting with a Qualified Security Assessor (QSA) is also recommended for accurate guidance.