- PCI DSS v4.0 (Annotated)
  - Principles
    - Requirements
    - Appendices
    - Annotations
  - PRINCIPLE PCI DSS REQUIREMENT: Build and Maintain a Secure Network and Systems
    - Requirement 1: Install and Maintain Network Security Controls
      - OVERVIEW
      - SECTIONS 1
        - REQUIREMENTS and TESTING PROCEDURES 1.1
          - DEFINED APPROACH REQUIREMENTS
          - CUSTOMIZED APPROACH OBJECTIVE
          - APPLICABILITY NOTES
          - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
          - DEFINED APPROACH REQUIREMENTS
          - CUSTOMIZED APPROACH OBJECTIVE
          - APPLICABILITY NOTES
          - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
        - REQUIREMENTS and TESTING PROCEDURES 1.2
          - DEFINED APPROACH REQUIREMENTS
          - CUSTOMIZED APPROACH OBJECTIVE
          - APPLICABILITY NOTES
          - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
          - DEFINED APPROACH REQUIREMENTS
          - CUSTOMIZED APPROACH OBJECTIVE
          - APPLICABILITY NOTES
          - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
          - DEFINED APPROACH REQUIREMENTS
          - CUSTOMIZED APPROACH OBJECTIVE
          - APPLICABILITY NOTES
          - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
          - DEFINED APPROACH REQUIREMENTS
          - CUSTOMIZED APPROACH OBJECTIVE

    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 1.3
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

        - REQUIREMENTS and TESTING PROCEDURES 1.4
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
        - REQUIREMENTS and TESTING PROCEDURES 1.5
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
- Requirement 2: Apply Secure Configurations to All System Components
    - OVERVIEW
    - SECTIONS 2
        - REQUIREMENTS and TESTING PROCEDURES 2.1
            - DEFINED APPROACH REQUIREMENTS
            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES

    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 2.2
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 2.3
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- PRINCIPLE PCI DSS REQUIREMENT: Protect Account Data
  - Requirement 3: Protect Stored Account Data
    - OVERVIEW
    - SECTIONS 3
      - REQUIREMENTS and TESTING PROCEDURES 3.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 3.2
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 3.3
        - DEFINED APPROACH REQUIREMENTS

        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
    - REQUIREMENTS and TESTING PROCEDURES x.y
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
    - REQUIREMENTS and TESTING PROCEDURES 3.4
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES

    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 3.5
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 3.6
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 3.7
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES

- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- PRINCIPLE PCI DSS REQUIREMENT: Protect Account Data
  - Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
    - OVERVIEW
    - SECTIONS 4
      - REQUIREMENTS and TESTING PROCEDURES 4.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 4.2
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE

- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- GUIDANCE
- PRINCIPLE PCI DSS REQUIREMENT: Maintain a Vulnerability Management Program
- Requirement 5: Protect All Systems and Networks from Malicious Software
- OVERVIEW
- SECTIONS 5
- REQUIREMENTS and TESTING PROCEDURES 5.1
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 5.2
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE

    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 5.3
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES x.y
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- PRINCIPLE PCI DSS REQUIREMENT: Maintain a Vulnerability Management Program
- Requirement 6: Develop and Maintain Secure Systems and Software
- OVERVIEW
- SECTIONS 6
- REQUIREMENTS and TESTING PROCEDURES 6.1
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 6.2
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS

- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 6.3
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 6.4
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES

    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 6.5
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures
  - Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know
    - OVERVIEW
    - SECTIONS 7
      - REQUIREMENTS and TESTING PROCEDURES 7.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 7.2
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES x.y
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE

                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
            - REQUIREMENTS and TESTING PROCEDURES 7.3
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
    - PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures
        - Requirement 8: Identify Users and Authenticate Access to System Components
            - OVERVIEW
            - SECTIONS 8
                - REQUIREMENTS and TESTING PROCEDURES 8.1
                - DEFINED APPROACH REQUIREMENTS

    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 8.1
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES

- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 8.3
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE

    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES x.y
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 8.4
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES

                - GUIDANCE
                    - DEFINED APPROACH REQUIREMENTS
                    - CUSTOMIZED APPROACH OBJECTIVE
                    - APPLICABILITY NOTES
                    - DEFINED APPROACH TESTING PROCEDURES
                - GUIDANCE
                    - DEFINED APPROACH REQUIREMENTS
                    - CUSTOMIZED APPROACH OBJECTIVE
                    - APPLICABILITY NOTES
                    - DEFINED APPROACH TESTING PROCEDURES
                - GUIDANCE
                - REQUIREMENTS and TESTING PROCEDURES 8.5
                    - DEFINED APPROACH REQUIREMENTS
                    - CUSTOMIZED APPROACH OBJECTIVE
                    - APPLICABILITY NOTES
                    - DEFINED APPROACH TESTING PROCEDURES
                - GUIDANCE
                - REQUIREMENTS and TESTING PROCEDURES 8.6
                    - DEFINED APPROACH REQUIREMENTS
                    - CUSTOMIZED APPROACH OBJECTIVE
                    - APPLICABILITY NOTES
                    - DEFINED APPROACH TESTING PROCEDURES
                - GUIDANCE
                    - DEFINED APPROACH REQUIREMENTS
                    - CUSTOMIZED APPROACH OBJECTIVE
                    - APPLICABILITY NOTES
                    - DEFINED APPROACH TESTING PROCEDURES
                - GUIDANCE
                    - DEFINED APPROACH REQUIREMENTS
                    - CUSTOMIZED APPROACH OBJECTIVE
                    - APPLICABILITY NOTES
                    - DEFINED APPROACH TESTING PROCEDURES
                - GUIDANCE
- PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures
    - Requirement 9: Restrict Physical Access to Cardholder Data
        - OVERVIEW
        - SECTIONS 9
            - REQUIREMENTS and TESTING PROCEDURES 9.1

  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 9.2
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 9.3
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE

    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 9.4
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 9.5
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES

- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- PRINCIPLE PCI DSS REQUIREMENT: Regularly Monitor and Test Networks
  - Requirement 10: Log and Monitor All Access to System Components and Cardholder Data
    - OVERVIEW
    - SECTIONS 10
      - REQUIREMENTS and TESTING PROCEDURES 10.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 10.2

    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES

- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 10.3
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 10.4
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS

        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
    - REQUIREMENTS and TESTING PROCEDURES 10.5
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
    - REQUIREMENTS and TESTING PROCEDURES 10.6
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
    - REQUIREMENTS and TESTING PROCEDURES 10.7
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE

- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- PRINCIPLE PCI DSS REQUIREMENT: Regularly Monitor and Test Networks
- Requirement 11: Test Security of Systems and Networks Regularly
- OVERVIEW
- SECTIONS 11
- REQUIREMENTS and TESTING PROCEDURES 11.1
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 11.2
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- DEFINED APPROACH REQUIREMENTS
- CUSTOMIZED APPROACH OBJECTIVE
- APPLICABILITY NOTES
- DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- REQUIREMENTS and TESTING PROCEDURES 11.3
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 11.4
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE

    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 11.5
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 11.6
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
- PRINCIPLE PCI DSS REQUIREMENT: Maintain an Information Security Policy
  - Requirement 12: Support Information Security with Organizational Policies and Programs
    - OVERVIEW
    - SECTIONS 12
      - REQUIREMENTS and TESTING PROCEDURES 12.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES 12.2
        - DEFINED APPROACH REQUIREMENTS

    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.3
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.4
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES

    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.5
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.6
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.7
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.8
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE

    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.9
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES 12.10
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES

- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- Appendix A Additonal PCI Requirements
  - OVERVIEW
  - SECTIONS A
- Appendix A Additonal PCI Requirements
  - Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers
    - OVERVIEW
    - SECTIONS A1
      - REQUIREMENTS and TESTING PROCEDURES A1.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES

- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
- REQUIREMENTS and TESTING PROCEDURES A1.2
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
  - DEFINED APPROACH REQUIREMENTS
  - CUSTOMIZED APPROACH OBJECTIVE
  - APPLICABILITY NOTES
  - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE

- Appendix A Additonal PCI Requirements
  - Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card- Present POS POI Terminal Connections
    - OVERVIEW
    - SECTIONS A2
      - REQUIREMENTS and TESTING PROCEDURES A2.1
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS

            - CUSTOMIZED APPROACH OBJECTIVE
            - APPLICABILITY NOTES
            - DEFINED APPROACH TESTING PROCEDURES
        - GUIDANCE
- Appendix A Additonal PCI Requirements
    - Appendix A3: Designated Entities Supplemental Validation (DESV)
        - OVERVIEW
        - SECTIONS A3
            - REQUIREMENTS and TESTING PROCEDURES A3.1
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
            - REQUIREMENTS and TESTING PROCEDURES A3.2
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES
            - GUIDANCE
                - DEFINED APPROACH REQUIREMENTS
                - CUSTOMIZED APPROACH OBJECTIVE
                - APPLICABILITY NOTES
                - DEFINED APPROACH TESTING PROCEDURES

- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES
    - DEFINED APPROACH TESTING PROCEDURES
- GUIDANCE
    - DEFINED APPROACH REQUIREMENTS
    - CUSTOMIZED APPROACH OBJECTIVE
    - APPLICABILITY NOTES

        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES A3.3
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES A3.4
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
      - REQUIREMENTS and TESTING PROCEDURES A3.5
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
      - GUIDANCE
- Appendix B Compensating Controls
  - OVERVIEW
    - REQUIREMENTS and TESTING PROCEDURES x.y
      - DEFINED APPROACH REQUIREMENTS

        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
    - REQUIREMENTS and TESTING PROCEDURES x.y
        - DEFINED APPROACH REQUIREMENTS
        - CUSTOMIZED APPROACH OBJECTIVE
        - APPLICABILITY NOTES
        - DEFINED APPROACH TESTING PROCEDURES
    - GUIDANCE
- Annotations Requirement 1
- Annotations Requirement 2
- Annotations Requirement 3
- Annotations Requirement 4
- Annotations Requirement 5
- Annotations Requirement 6
- Annotations Requirement 7
- Annotations Requirement 8
- Annotations Requirement 9
- Annotations Requirement 10
- Annotations Requirement 11
- Annotations Requirement 12

PCI DSS v4.0 (Annotated)

This annotated reference is based on information sourced from PCI SSC and the PCI DSS v4.0 Resource Hub

Principles

PRINCIPLE PCI DSS REQUIREMENT: Build and Maintain a Secure Network and Systems

PRINCIPLE PCI DSS REQUIREMENT: Protect Account Data

PRINCIPLE PCI DSS REQUIREMENT: Maintain a Vulnerability Management Program

PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures

PRINCIPLE PCI DSS REQUIREMENT: Regularly Monitor and Test Networks

PRINCIPLE PCI DSS REQUIREMENT: Maintain an Information Security Policy

Appendix A Additonal PCI Requirements

Appendix B Compensating Controls

Appendix C Compensating Controls Worksheet

Appendix D Customized Approach

Appendix E Sample Templates to Support Customized Approach

Appendix F Leveraging the PCI Software Security Framework to Support Requirement 6

Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms

Requirements

Requirement 1: Install and Maintain Network Security Controls

Requirement 2: Apply Secure Configurations to All System Components

Requirement 3: Protect Stored Account Data

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Requirement 5: Protect All Systems and Networks from Malicious Software

Requirement 6: Develop and Maintain Secure Systems and Software

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Requirement 8: Identify Users and Authenticate Access to System Components

Requirement 9: Restrict Physical Access to Cardholder Data

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Requirement 11: Test Security of Systems and Networks Regularly

Requirement 12: Support Information Security with Organizational Policies and Programs

Appendices

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections

Appendix A3: Designated Entities Supplemental Validation (DESV)

Appendix B: Compensating Controls

Appendix C: Compensating Controls Worksheet

Appendix D: Customized Approach

Appendix E: Sample Templates to Support Customized Approach

Appendix F: Leveraging the PCI Software Security Framework to Support Requirement 6

Appendix G: PCI DSS Glossary of Terms, Abbreviations, and Acronyms

Annotations

Annotation Requirement 1

Annotation Requirement 2

Annotation Requirement 3

Annotation Requirement 4

Annotation Requirement 5

Annotation Requirement 6

Annotation Requirement 7

Annotation Requirement 8

Annotation Requirement 9

Annotation Requirement 10

Annotation Requirement 11

Annotation Requirement 12

PRINCIPLE PCI DSS REQUIREMENT: Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

OVERVIEW

Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.

NSCs examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.

Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

NSCs are used to control traffic within an entity's own networks—for example, between highly sensitive and less sensitive areas—and also to protect the entity's resources from exposure to untrusted networks. The cardholder data environment (CDE) is an example of a more sensitive area within an entity's network. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into sensitive systems. NSCs provide a key protection mechanism for any computer network.

Common examples of untrusted networks include the Internet, dedicated connections such as business-to-business communication channels, wireless networks, carrier networks (such as cellular), third-party networks, and other sources outside the entity's ability to control. Furthermore, untrusted networks also include corporate networks that are considered out-of-scope for PCI DSS, because they are not assessed, and therefore must

be treated as untrusted because the existence of security controls has not been verified. While an entity may consider an internal network to be trusted from an infrastructure perspective, if a network is out of scope for PCI DSS, that network must be considered untrusted for PCI DSS.

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 1

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.

1.2 Network security controls (NSCs) are configured and maintained.

1.3 Network access to and from the cardholder data environment is restricted.

1.4 Network connections between trusted and untrusted networks are controlled.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

requirement 1 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 1.1

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.

DEFINED APPROACH REQUIREMENTS

1.1.1 All security policies and operational procedures that are identified in Requirement 1 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management’s intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 1.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 1. While it is important to define the specific policies or procedures called out in Requirement 1, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For these reasons, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity’s security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.

1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

sections 1 | top

REQUIREMENTS and TESTING PROCEDURES 1.2

1.2 Network security controls (NSCs) are configured and maintained.

DEFINED APPROACH REQUIREMENTS

1.2.1 Configuration standards for NSC rulesets are:

- Defined.
- Implemented.
- Maintained.

CUSTOMIZED APPROACH OBJECTIVE

The way that NSCs are configured and operate are defined and consistently applied.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.2.1.a Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.

1.2.1.b Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.

GUIDANCE

Purpose

The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset).

Good Practice

These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network.

Definitions

NSCs are key components of a network architecture. Most commonly, NSCs are used at the boundaries of the CDE to control network traffic flowing inbound and outbound from the CDE. Configuration standards outline an entity’s minimum requirements for the configuration of its NSCs

Examples

Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.

DEFINED APPROACH REQUIREMENTS

1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

CUSTOMIZED APPROACH OBJECTIVE

Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.

APPLICABILITY NOTES

Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.

DEFINED APPROACH TESTING PROCEDURES

1.2.2.a Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.

1.2.2.b Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.

1.2.2.c Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.

GUIDANCE

Good Practice

Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected.

To avoid having to address security issues introduced by a change, all changes should be approved prior to being implemented and verified after the change is implemented. Once

approved and verified, network documentation should be updated to include the changes to prevent inconsistencies between network documentation and the actual configuration.

DEFINED APPROACH REQUIREMENTS

1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.

CUSTOMIZED APPROACH OBJECTIVE

A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.

APPLICABILITY NOTES

A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.

DEFINED APPROACH TESTING PROCEDURES

1.2.3.a Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.

1.2.3.b Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.

GUIDANCE

Purpose

Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise.

A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE.

Good Practice

All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams:

- All locations, including retail locations, data centers, corporate locations, cloud providers, etc.
- Clear labeling of all network segments.
- All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version).
- All in-scope system components, including NSCs, web app firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc.
- Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism.
- Date of last update, and names of people that made and approved the updates.
- A legend or key to explain the diagram.

DEFINED APPROACH REQUIREMENTS

1.2.4 An accurate data-flow diagram(s) is maintained that meets the following:

- Shows all account data flows across systems and networks.
- Updated as needed upon changes to the environment.

CUSTOMIZED APPROACH OBJECTIVE

A representation of all transmissions of account data between system components and across network segments is maintained and available.

APPLICABILITY NOTES

A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement

DEFINED APPROACH TESTING PROCEDURES

1.2.4.a Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement.

1.2.4.b Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.

GUIDANCE

Purpose

An up-to-date, readily available data-flow diagram helps an organization understand and keep track of the scope of its environment by showing how account data flows across networks and between individual systems and devices.

Maintaining an up-to-date data-flow diagram(s) prevents account data from being overlooked and unknowingly left unsecured.

Good Practice

The data-flow diagram should include all connection points where account data is received into and sent out of the network, including connections to open, public networks, application processing flows, storage, transmissions between systems and networks, and file backups.

The data-flow diagram is meant to be in addition to the network diagram and should reconcile with and augment the network diagram. As a best practice, entities can consider including the following in their data-flow diagrams:

- All processing flows of account data, including authorization, capture, settlement, chargeback, and refunds.
- All distinct acceptance channels, including card-present, card-not-present, and e-commerce.
- All types of data receipt or transmission, including any involving hard copy/paper media.
- The flow of account data from the point where it enters the environment, to its final disposition.
- Where account data is transmitted and processed, where it is stored, and whether storage is short term or long term.
- The source of all account data received (for example, customers, third party, etc.), and any entities with which account data is shared.
- Date of last update, and names of people that made and approved the updates.

DEFINED APPROACH REQUIREMENTS

1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.2.5.a Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.

1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.

GUIDANCE

Purpose

Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed.

Good Practice

The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.

DEFINED APPROACH REQUIREMENTS

1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.

CUSTOMIZED APPROACH OBJECTIVE

The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.2.6.a Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.

1.2.6.b Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.

GUIDANCE

Purpose

Compromises take advantage of insecure network configurations.

Good Practice

If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity.

Definitions

Examples

Further Information

For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (for example, from NIST, ENISA, OWASP).

DEFINED APPROACH REQUIREMENTS

1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.

CUSTOMIZED APPROACH OBJECTIVE

NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.2.7.a Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.

1.2.7.b Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.

1.2.7.c Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.

GUIDANCE

Purpose

Such a review gives the organization an opportunity to clean up any unneeded, outdated, or incorrect rules and configurations which could be utilized by an unauthorized person. Furthermore, it ensures that all rules and configurations allow only authorized services, protocols, and ports that match the documented business justifications.

Good Practice

This review, which can be implemented using manual, automated, or system-based methods, is intended to confirm that the settings that manage traffic rules, what is allowed in and out of the network, match the approved configurations. The review should provide confirmation that all permitted access has a justified business reason. Any discrepancies or uncertainties about a rule or configuration should be escalated for resolution.

While this requirement specifies that this review occur at least once every six months, organizations with a high volume of changes to their network configurations may wish to consider performing reviews more frequently to ensure that the configurations continue to meet the needs of the business.

Definitions

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

1.2.8 Configuration files for NSCs are:

- Secured from unauthorized access.
- Kept consistent with active network configurations

CUSTOMIZED APPROACH OBJECTIVE

NSCs cannot be defined or modified using untrusted configuration objects (including files).

APPLICABILITY NOTES

Any file or setting used to configure or synchronize NSCs is considered to be a “configuration file.” This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.

DEFINED APPROACH TESTING PROCEDURES

1.2.8 Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

To prevent unauthorized configurations from being applied to the network, stored files with configurations for network controls need to be kept up to date and secured against unauthorized changes.

Keeping configuration information current and secure ensures that the correct settings for NSCs are applied whenever the configuration is run.

Good Practice

Definitions

Examples

If the secure configuration for a router is stored in non-volatile memory, when that router is restarted or rebooted, these controls should ensure that its secure configuration is reinstated.

Further Information

sections 1 | top

REQUIREMENTS and TESTING PROCEDURES 1.3

1.3 Network access to and from the cardholder data environment is restricted.

DEFINED APPROACH REQUIREMENTS

1.3.1 Inbound traffic to the CDE is restricted as follows:

- To only traffic that is necessary.
- All other traffic is specifically denied

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized traffic cannot enter the CDE.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.3.1.a Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.

1.3.1.b Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

This requirement aims to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner.

Good Practice

All traffic inbound to the CDE, regardless of where it originates, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to ensure traffic is restricted to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.

Definitions

Examples

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed— for example, by using an explicit "deny all" or implicit deny after allow statement —helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.

Further Information

DEFINED APPROACH REQUIREMENTS

1.3.2 Outbound traffic from the CDE is restricted as follows:

- To only traffic that is necessary.
- All other traffic is specifically denied.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized traffic cannot leave the CDE.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.3.2.a Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement.

1.3.2.b Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

This requirement aims to prevent malicious individuals and compromised system components within the entity's network from communicating with an untrusted external host.

Good Practice

All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.

Definitions

Examples

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed— for example, by using an explicit "deny all" or implicit deny after allow statement —helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.

Further Information

DEFINED APPROACH REQUIREMENTS

1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:

- All wireless traffic from wireless networks into the CDE is denied by default.
- Only wireless traffic with an authorized business purpose is allowed into the CDE.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.3.3 Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.

Good Practice

Definitions

Examples

Further Information

REQUIREMENTS and TESTING PROCEDURES 1.4

1.4 Network connections between trusted and untrusted networks are controlled.

DEFINED APPROACH REQUIREMENTS

1.4.1 NSCs are implemented between trusted and untrusted networks.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.4.1.a Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.

1.4.1.b Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.

GUIDANCE

Purpose

Implementing NSCs at every connection coming into and out of trusted networks allows the entity to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.

Good Practice

Definitions

Examples An entity could implement a DMZ, which is a part of the network that manages connections between an untrusted network (for examples of untrusted networks refer to the Requirement 1 Overview) and services that an organization needs to have available to the public, such as a web server. Please note that if an entity's DMZ processes or transmits account data (for example, e-commerce website), it is also considered a CDE.

Further Information

DEFINED APPROACH REQUIREMENTS

1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to:

- Communications with system components that are authorized to provide publicly accessible services, protocols, and ports.
- Stateful responses to communications initiated by system components in a trusted network.
- All other traffic is denied.

CUSTOMIZED APPROACH OBJECTIVE

Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network

APPLICABILITY NOTES

The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.

DEFINED APPROACH TESTING PROCEDURES

1.4.2 Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Ensuring that public access to a system component is specifically authorized reduces the risk of system components being unnecessarily exposed to untrusted networks.

Good Practice

System components that provide publicly accessible services, such as email, web, and DNS servers, are the most vulnerable to threats originating from untrusted networks. Ideally, such systems are placed within a dedicated trusted network that is public facing (for

example, a DMZ) but that is separated via NSCs from more sensitive internal systems, which helps protect the rest of the network in the event these externally accessible systems are compromised. This functionality is intended to prevent malicious actors from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.

Where this functionality is provided as a built-in feature of an NSC, the entity should ensure that its configurations do not result in the functionality being disabled or bypassed.

Definitions

Maintaining the "state" (or status) for each connection into a network means the NSC “knows” whether an apparent response to a previous connection is a valid, authorized response (since the NSC retains each connection’s status) or whether it is malicious traffic trying to fool the NSC into allowing the connection.

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

CUSTOMIZED APPROACH OBJECTIVE

Packets with forged IP source addresses cannot enter a trusted network.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.4.3 Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

GUIDANCE

Purpose

Filtering packets coming into the trusted network helps to, among other things, ensure packets are not “spoofed” to appear as if they are coming from an organization’s own

internal network. For example, anti-spoofing measures prevent internal addresses originating from the Internet from passing into the DMZ.

Good Practice

Products usually come with anti-spoofing set as a default and may not be configurable. Entities should consult the vendor's documentation for more information.

Definitions

Examples

Normally, a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet originated. Malicious individuals will often try to spoof (or imitate) the sending IP address to fool the target system into believing the packet is from a trusted source.

Further Information

DEFINED APPROACH REQUIREMENTS

1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.

CUSTOMIZED APPROACH OBJECTIVE

Stored cardholder data cannot be accessed from untrusted networks.

APPLICABILITY NOTES

This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).

DEFINED APPROACH TESTING PROCEDURES

1.4.4.a Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.

1.4.4.b Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.

GUIDANCE

Purpose

Cardholder data that is directly accessible from an untrusted network, for example, because it is stored on a system within the DMZ or in a cloud database service, is easier for an external attacker to access because there are fewer defensive layers to penetrate. Using NSCs to ensure that system components that store cardholder data (such as a database or a file) can only be directly accessed from trusted networks can prevent unauthorized network traffic from reaching the system component.

Good Practice

Definitions

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.

CUSTOMIZED APPROACH OBJECTIVE

Internal network information is protected from unauthorized disclosure.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

1.4.5.a Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.

1.4.5.b Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.

GUIDANCE

Purpose

Restricting the disclosure of internal, private, and local IP addresses is useful to prevent a hacker from obtaining knowledge of these IP addresses and using that information to access the network.

Good Practice

Methods used to meet the intent of this requirement may vary, depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.

Definitions

Examples

Methods to obscure IP addressing may include, but are not limited to:

- IPv4 Network Address Translation (NAT).
- Placing system components behind proxy servers/NSCs.
- Removal or filtering of route advertisements for internal networks that use registered addressing.
- Internal use of RFC 1918 (IPv4) or use IPv6 privacy extension (RFC 4941) when initiating outgoing sessions to the internet.

Further Information

sections 1 | top

REQUIREMENTS and TESTING PROCEDURES 1.5

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

DEFINED APPROACH REQUIREMENTS

1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows:

- Specific configuration settings are defined to prevent threats being introduced into the entity's network.
- Security controls are actively running.
- Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

CUSTOMIZED APPROACH OBJECTIVE

Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.

APPLICABILITY NOTES

These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.

DEFINED APPROACH TESTING PROCEDURES

1.5.1.a Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement.

1.5.1.b Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats.

Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example,

firewalls, network- based heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network.

Good Practice

The specific configuration settings are determined by the entity and should be consistent with its network security policies and procedures. Where there is a legitimate need to temporarily disable security controls on a company-owned or employee-owned device that connects to both an untrusted network and the CDE—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action is understood and approved by an appropriate management representative.

Any disabling or altering of these security controls, including on administrators' own devices, is performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable security controls on their own computers, but there should be alerting mechanisms in place when such controls are disabled and follow up that occurs to ensure processes were followed.

Definitions

Examples

Practices include forbidding split-tunneling of VPNs for employee-owned or corporate-owned mobile devices and requiring that such devices boot up into a VPN.

Further Information

sections 1 | top

Requirement 2: Apply Secure Configurations to All System Components

OVERVIEW

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary

software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 2

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.

2.2 System components are configured and managed securely.

2.3 Wireless environments are configured and managed securely.

requirement 2 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 2.1

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.

DEFINED APPROACH REQUIREMENTS

2.1.1 All security policies and operational procedures that are identified in Requirement 2 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 2 are managed in accordance with all

elements specified in this requirement.

GUIDANCE

Purpose

Requirement 2.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 2. While it is important to define the specific policies or procedures called out in Requirement 2, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle

Definitions

Security policies define the entity's security objectives and principles.

Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 2 are documented and assigned.

2.1.2.b Interview personnel with responsibility for performing activities in Requirement 2 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 2 | top

REQUIREMENTS and TESTING PROCEDURES 2.2

2.2 System components are configured and managed securely.

DEFINED APPROACH REQUIREMENTS

2.2.1 Configuration standards are developed, implemented, and maintained to:

- Cover all system components.
- Address all known security vulnerabilities.

- Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.
- Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.
- Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.

CUSTOMIZED APPROACH OBJECTIVE

All system components are configured securely and consistently and in accordance with industry- accepted hardening standards or vendor recommendations.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.2.1.a Examine system configuration standards to verify they define processes that include all elements specified in this requirement.

2.2.1.b Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.

2.2.1.c Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.

GUIDANCE

Purpose

There are known weaknesses with many operating systems, databases, network devices, software, applications, container images, and other devices used by an entity or within an entity’s environment. There are also known ways to configure these system components to fix security vulnerabilities. Fixing security vulnerabilities reduces the opportunities available to an attacker.

By developing standards, entities ensure their system components will be configured consistently and securely, and address the protection of devices for which full hardening may be more difficult.

Good Practice

Keeping up to date with current industry guidance will help the entity maintain secure configurations.

The specific controls to be applied to a system will vary and should be appropriate for the type and function of the system. Numerous security organizations have established system-hardening guidelines and recommendations, which advise how to correct common, known weaknesses.

Definitions

Examples

Further Information

Sources for guidance on configuration standards include but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance, and product vendors.

DEFINED APPROACH REQUIREMENTS

2.2.2 Vendor default accounts are managed as follows:

- If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
- If the vendor default account(s) will not be used, the account is removed or disabled

CUSTOMIZED APPROACH OBJECTIVE

System components cannot be accessed using default passwords.

APPLICABILITY NOTES

This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults.

This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.

DEFINED APPROACH TESTING PROCEDURES

2.2.2.a Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.

2.2.2.b Examine vendor documentation and observe a system administrator logging on using vendor default accounts to verify accounts are implemented in accordance with all elements specified in this requirement.

2.2.2.c Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.

GUIDANCE

Purpose

Malicious individuals often use vendor default account names and passwords to compromise operating systems, applications, and the systems on which they are installed. Because these default settings are often published and are well known, changing these settings will make systems less vulnerable to attack.

Good Practice

All vendor default accounts should be identified, and their purpose and use understood. It is important to establish controls for application and system accounts, including those used to deploy and maintain cloud services so that they do not use default passwords and are not usable by unauthorized individuals.

Where a default account is not intended to be used, changing the default password to a unique password that meets PCI DSS Requirement 8.3.6, removing any access to the default account, and then disabling the account, will prevent a malicious individual from re-enabling the account and gaining access with the default password.

Using an isolated staging network to install and configure new systems is recommended and can also be used to confirm that default credentials have not been introduced into production environments.

Definitions

Examples

Defaults to be considered include user IDs, passwords, and other authentication credentials commonly used by vendors in their products.

Further Information

REQUIREMENTS and TESTING PROCEDURES

DEFINED APPROACH REQUIREMENTS

2.2.3 Primary functions requiring different security levels are managed as follows:

- Only one primary function exists on a system component, OR
- Primary functions with differing security levels that exist on the same system component are isolated from each other, OR
- Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.

CUSTOMIZED APPROACH OBJECTIVE

Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.2.3.a Examine system configuration standards to verify they include managing primary functions requiring different security levels as specified in this requirement.

2.2.3.b Examine system configurations to verify that primary functions requiring different security levels are managed per one of the ways specified in this requirement.

2.2.3.c Where virtualization technologies are used, examine the system configurations to verify that system functions requiring different security levels are managed in one of the following ways:

- Functions with differing security needs do not co-exist on the same system component.
- Functions with differing security needs that exist on the same system component are isolated from each other.
- Functions with differing security needs on the same system component are all secured to the level required by the function with the highest security need.

GUIDANCE

Purpose

Systems containing a combination of services, protocols, and daemons for their primary function will have a security profile appropriate to allow that function to operate effectively. For example, systems that need to be directly connected to the Internet would have a particular profile, like a DNS server, web server, or an e-commerce server. Conversely, other system components may operate a primary function comprising a different set of services, protocols, and daemons that performs functions that an entity does not want exposed to the Internet. This requirement aims to ensure that different functions do not impact the security profiles of other services in a way which may cause them to operate at a higher or lower security level.

Good Practice

Ideally, each function should be placed on different system components. This can be achieved by implementing only one primary function on each system component. Another option is to isolate primary functions on the same system component that have different security levels, for example, isolating web servers (which need to be directly connected to the Internet) from application and database servers.

If a system component contains primary functions that need different security levels, a third option is to implement additional controls to ensure that the resultant security level of the primary function(s) with higher security needs is not reduced by the presence of the lower security primary functions. Additionally, the functions with a lower security level should be isolated and/or secured to ensure they cannot access or affect the resources of another system function, and do not introduce security weaknesses to other functions on the same server.

Functions of differing security levels may be isolated by either physical or logical controls. For example, a database system should not also be hosting web services unless using controls like virtualization technologies to isolate and contain the functions into separate sub-systems. Another example is using virtual instances or providing dedicated memory access by system function.

Where virtualization technologies are used, the security levels should be identified and managed for each virtual component. Examples of considerations for virtualized environments include:

- The function of each application, container, or virtual server instance.
- How virtual machines (VMs) or containers are stored and secured.

Definitions

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.

CUSTOMIZED APPROACH OBJECTIVE

System components cannot be compromised by exploiting unnecessary functionality present in the system component.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.2.4.a Examine system configuration standards to verify necessary system services, protocols, and daemons are identified and documented.

2.2.4.b Examine system configurations to verify the following:

- All unnecessary functionality is removed or disabled.
- Only required functionality, as documented in the configuration standards, is enabled.

GUIDANCE

Purpose

Unnecessary services and functions can provide additional opportunities for malicious individuals to gain access to a system. By removing or disabling all unnecessary services, protocols, daemons, and functions, organizations can focus on securing the functions that are required and reduce the risk that unknown or unnecessary functions will be exploited

Good Practice

There are many protocols that could be enabled by default that are commonly used by malicious individuals to compromise a network. Disabling or removing all services, functions, and protocols that are not used minimizes the potential attack surface—for example, by removing or disabling an unused FTP or web server.

Definitions

Examples

Unnecessary functionality may include, but is not limited to scripts, drivers, features, subsystems, file systems, interfaces (USB and Bluetooth), and unnecessary web servers

Further Information

DEFINED APPROACH REQUIREMENTS

2.2.5 If any insecure services, protocols, or daemons are present:

- Business justification is documented.
- Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.

CUSTOMIZED APPROACH OBJECTIVE

System components cannot be compromised by exploiting insecure services, protocols, or daemons

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.2.5.a If any insecure services, protocols, or daemons are present, examine system configuration standards and interview personnel to verify they are managed and implemented in accordance with all elements specified in this requirement.

2.2.5.b If any insecure services, protocols, or daemons, are present, examine configuration settings to verify that additional security features are implemented to reduce the risk of using insecure services, daemons, and protocols.

GUIDANCE

Purpose

Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to exploit common points of compromise within a network

Good Practice

Enabling security features before new system components are deployed will prevent insecure configurations from being introduced into the environment. Some vendor solutions may provide additional security functions to assist with securing an insecure process.

Definitions

Examples

Further Information

For guidance on services, protocols, or daemons considered to be insecure, refer to industry standards and guidance (for example, as published by NIST, ENISA, and OWASP).

DEFINED APPROACH REQUIREMENTS

2.2.6 System security parameters are configured to prevent misuse.

CUSTOMIZED APPROACH OBJECTIVE

System components cannot be compromised because of incorrect security parameter configuration.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.2.6.a Examine system configuration standards to verify they include configuring system security parameters to prevent misuse.

2.2.6.b Interview system administrators and/or security managers to verify they have knowledge of common security parameter settings for system components.

2.2.6.c Examine system configurations to verify that common security parameters are set appropriately and in accordance with the system configuration standards.

GUIDANCE

Purpose

Correctly configuring security parameters provided in system components takes advantage of the capabilities of the system component to defeat malicious attacks.

Good Practice

System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use.

For systems to be configured securely, personnel responsible for configuration and/or administering systems should be knowledgeable in the specific security parameters and settings that apply to the system. Considerations should also include secure settings for parameters used to access cloud portals.

Definitions

Examples

Further Information

Refer to vendor documentation and industry references noted in Requirement 2.2.1 for information about applicable security parameters for each type of system.

DEFINED APPROACH REQUIREMENTS

2.2.7 All non-console administrative access is encrypted using strong cryptography.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.

APPLICABILITY NOTES

This includes administrative access via browser- based interfaces and application programming interfaces (APIs).

DEFINED APPROACH TESTING PROCEDURES

2.2.7.a Examine system configuration standards to verify they include encrypting all non-console administrative access using strong cryptography.

2.2.7.b Observe an administrator log on to system components and examine system configurations to verify that non-console administrative access is managed in accordance with this requirement.

2.2.7.c Examine settings for system components and authentication services to verify that insecure remote login services are not available for non- console administrative access.

2.2.7.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.

GUIDANCE

Purpose

If non-console (including remote) administration does not use encrypted communications, administrative authorization factors (such as IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data.

Good Practice

Whichever security protocol is used, it should be configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates, supporting only strong encryption, and not supporting fallback to weaker, insecure protocols or methods.

Definitions

Examples

Cleartext protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. Non-console access may be facilitated by technologies that provide alternative access to systems, including but not limited to, out-of-band (OOB), lights-out management (LOM), Intelligent Platform Management Interface (IPMI), and keyboard, video, mouse (KVM) switches with remote capabilities. These and other non-console access technologies and methods must be secured with strong cryptography.

Further Information Refer to industry standards and best practices such as NIST SP 800-52 and SP 800-57.

sections 2 | top

REQUIREMENTS and TESTING PROCEDURES 2.3

2.3 Wireless environments are configured and managed securely.

DEFINED APPROACH REQUIREMENTS

2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:

- Default wireless encryption keys.
- Passwords on wireless access points.
- SNMP defaults.
- Any other security-related wireless vendor defaults.

CUSTOMIZED APPROACH OBJECTIVE

Wireless networks cannot be accessed using vendor default passwords or default configurations.

APPLICABILITY NOTES

This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.

DEFINED APPROACH TESTING PROCEDURES

2.3.1.a Examine policies and procedures and interview responsible personnel to verify that processes are defined for wireless vendor defaults to either change them upon installation or to confirm them to be secure in accordance with all elements of this requirement.

2.3.1.b Examine vendor documentation and observe a system administrator logging into wireless devices to verify:

- SNMP defaults are not used.
- Default passwords/passphrases on wireless access points are not used.

2.3.1.c Examine vendor documentation and wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.

GUIDANCE

Purpose

If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network.

Good Practice

Wireless passwords should be constructed so that they are resistant to offline brute force attacks.

Definitions

Examples

Further Information

sections 2 | top

DEFINED APPROACH REQUIREMENTS

2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:

- Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.
- Whenever a key is suspected of or known to be compromised.

CUSTOMIZED APPROACH OBJECTIVE

Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

2.3.2 Interview responsible personnel and examine key-management documentation to verify that wireless encryption keys are changed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Changing wireless encryption keys whenever someone with knowledge of the key leaves the organization or moves to a role that no longer requires knowledge of the key, helps keep knowledge of keys limited to only those with a business need to know.

Also, changing wireless encryption keys whenever a key is suspected or known to be comprised makes a wireless network more resistant to compromise.

Good Practice

This goal can be accomplished in multiple ways, including periodic changes of keys, changing keys via a defined “joiners-movers-leavers” (JML) process, implementing

additional technical controls, and not using fixed pre-shared keys.

In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan at Requirement 12.10.1.

Definitions

Examples

Further Information

sections 2 | top

PRINCIPLE PCI DSS REQUIREMENT: Protect Account Data

Requirement 3: Protect Stored Account Data

OVERVIEW

Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as e-mail and instant messaging.

If account data is present in non-persistent memory (for example, RAM, volatile memory), encryption of account data is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS Requirements will apply including encryption of stored data.

Requirement 3 applies to protection of stored account data unless specifically called out in an individual requirement.

Refer to Appendix G for definitions of "strong cryptography" and other PCI DSS terms.

SECTIONS 3

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.2 Storage of account data is kept to a minimum.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.

3.5 Primary account number (PAN) is secured wherever it is stored.

3.6 Cryptographic keys used to protect stored account data are secured.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

requirement 3 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 3.1

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

DEFINED APPROACH REQUIREMENTS

3.1.1 All security policies and operational procedures that are identified in Requirement 3 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 3.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 3. While it is important to define the specific policies or procedures called out in Requirement 3, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.1.2.a Examine documentation to verify that descriptions of roles and responsibilities performing activities in Requirement 3 are documented and assigned.

3.1.2.b Interview personnel with responsibility for performing activities in Requirement 3 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES 3.2

3.2 Storage of account data is kept to a minimum.

DEFINED APPROACH REQUIREMENTS

3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

- Coverage for all locations of stored account data.
- Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
- Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
- Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
- Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
- A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

CUSTOMIZED APPROACH OBJECTIVE

Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.

APPLICABILITY NOTES

Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted.

The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.2.1.a Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement.

3.2.1.b Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy.

3.2.1.c Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.

GUIDANCE

Purpose

A formal data retention policy identifies what data needs to be retained, for how long, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only account data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code.

The storage of SAD data prior to the completion of the authorization process is also included in the data retention and disposal policy so that storage of this sensitive data is kept to minimum, and only retained for the defined amount of time.

Good Practice

When identifying locations of stored account data, consider all processes and personnel with access to the data, as data could have been moved and stored in different locations than originally defined. Storage locations that are often overlooked include backup and archive systems, removable data storage devices, paper-based media, and audio recordings.

To define appropriate retention requirements, an entity first needs to understand its own business needs as well as any legal or regulatory obligations that apply to its industry or to the type of data being retained. Implementing an automated process to ensure data is automatically and securely deleted upon its defined retention limit can help ensure that account data is not retained beyond what is necessary for business, legal, or regulatory purposes.

Methods of eliminating data when it exceeds the retention period include secure deletion to complete removal of the data or rendering it unrecoverable and unable to be reconstructed. Identifying and securely eliminating stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated, manual, or a combination of both.

The deletion function in most operating systems is not “secure deletion” as it allows deleted data to be recovered, so instead, a dedicated secure deletion function or application must be used to make data unrecoverable.

Remember, if you don't need it, don't store it!

Definitions

Examples

An automated, programmatic procedure could be run to locate and remove data, or a manual review of data storage areas could be performed. Whichever method is used, it is a good idea to monitor the process to ensure it is completed successfully, and that the results are recorded and validated as being complete. Implementing secure deletion methods ensures that the data cannot be retrieved when it is no longer needed.

Further Information

See *NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.*

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES 3.3

3.3 Sensitive authentication data (SAD) is not stored after authorization.

DEFINED APPROACH REQUIREMENTS

3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

This requirement does not apply to issuers and companies that support issuing services (where SAD is needed for a legitimate issuing business need) and have a business justification to store the sensitive authentication data.

Refer to Requirement 3.3.3 for additional requirements specifically for issuers.

Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.

DEFINED APPROACH TESTING PROCEDURES

3.3.1.a If SAD is received, examine documented policies, procedures, and system configurations to verify the data is not retained after authorization.

3.3.1.b If SAD is received, examine the documented procedures and observe the secure data deletion processes to verify the data is rendered unrecoverable upon completion of the authorization process.

GUIDANCE

Purpose

SAD is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Therefore, the storage of SAD upon completion of the authorization process is prohibited.

Good Practice

Definitions

The authorization process completes when a merchant receives a transaction response (for example, an approval or decline).

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

In the normal course of business, the following data elements from the track may need to be retained:

- Cardholder name.
- Primary account number (PAN).

- Expiration date.
- Service code. To minimize risk, store securely only these data elements as needed for business.

DEFINED APPROACH TESTING PROCEDURES

3.3.1.1 Examine data sources to verify that the full contents of any track are not stored upon completion of the authorization process.

GUIDANCE

Purpose

If full contents of any track (from the magnetic stripe on the back of a card if present, equivalent data contained on a chip, or elsewhere) is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions.

Good Practice

Definitions

Full track data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Each track contains a number of data elements, and this requirement specifies only those that may be retained post-authorization.

Examples

Data sources to review to ensure that the full contents of any track are not retained upon completion of the authorization process include, but are not limited to:

- Incoming transaction data.
- All logs (for example, transaction, history, debugging, error).
- History files.
- Trace files.
- Database schemas.
- Contents of databases, and on-premise and cloud data stores.
- Any existing memory/crash dump files.

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.3.1.2 The card verification code is not retained upon completion of the authorization process.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.

DEFINED APPROACH TESTING PROCEDURES

3.3.1.2 Examine data sources, to verify that the card verification code is not stored upon completion of the authorization process.

GUIDANCE

Purpose

If card verification code data is stolen, malicious individuals can execute fraudulent Internet and mail-order/telephone-order (MO/TO) transactions. Not storing this data reduces the probability of it being compromised.

Good Practice

Definitions

Examples

If card verification codes are stored on paper media prior to completion of authorization, a method of erasing or covering the codes should prevent them from being read after authorization is complete. Example methods of rendering the codes unreadable include removing the code with scissors and applying a suitably opaque and un-removable marker over the code.

Data sources to review to ensure that the card verification code is not retained upon completion of the authorization process include, but are not limited to:

- Incoming transaction data.
- All logs (for example, transaction, history, debugging, error).

- History files.
- Trace files.
- Database schemas.
- Contents of databases, and on-premise and cloud data stores.
- Any existing memory/crash dump files.

Further Information

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES x.y

DEFINED APPROACH REQUIREMENTS

3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.

DEFINED APPROACH TESTING PROCEDURES

3.3.1.3 Examine data sources, to verify that PINs and PIN blocks are not stored upon completion of the authorization process.

GUIDANCE

Purpose

PIN and PIN blocks should be known only to the card owner or entity that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based transactions (for example, in-store purchases and ATM withdrawals). Not storing this data reduces the probability of it being compromised.

Good Practice

Definitions

Examples

Data sources to review to ensure that PIN and PIN blocks are not retained upon completion of the authorization process include, but are not limited to:

- Incoming transaction data.
- All logs (for example, transaction, history, debugging, error).
- History files.
- Trace files.
- Database schemas.
- Contents of databases, and on-premise and cloud data stores.
- Any existing memory/crash dump files.

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact the organizations of interest for any additional criteria.

This requirement applies to all storage of SAD, even if no PAN is present in the environment.

Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization.

This requirement does not apply to issuers and companies that support issuing services where there is a legitimate issuing business justification to store SAD). Refer to Requirement 3.3.3 for requirements specifically for issuers.

This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.3.2 Examine data stores, system configurations, and/or vendor documentation to verify that all SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.

GUIDANCE

Purpose

SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions

Good Practice

Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.

Definitions

The authorization process is completed as soon as the response to an authorization request response—that is, an approval or decline—is received.

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is:

- Limited to that which is needed for a legitimate issuing business need and is secured.
- Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.

CUSTOMIZED APPROACH OBJECTIVE

Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access.

APPLICABILITY NOTES

This requirement applies only to issuers and companies that support issuing services and store sensitive authentication data. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data.

PCI DSS requirements are intended for all entities that store, process, or transmit account data, including issuers. The only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements.

The bullet above (for encrypting stored SAD with strong cryptography) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.3.3 and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.3.3.a Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data: Examine documented policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.

3.3.3.b Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data: Examine data stores and system configurations to verify that the sensitive authentication data is stored securely.

GUIDANCE

Purpose

SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions.

Good Practice

Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.

Definitions

Legitimate issuing business need means that the data is needed to facilitate the issuing business process.

Examples

Further Information

Refer to *ISO/DIS 9564-5 Financial services — Personal Identification Number (PIN) management and security — Part 5: Methods for the generation, change, and verification of PINs and card security data using the advanced encryption standard.*

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES 3.4

3.4 Access to displays of full PAN and ability to copy PAN is restricted.

DEFINED APPROACH REQUIREMENTS

3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.

CUSTOMIZED APPROACH OBJECTIVE

PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.

APPLICABILITY NOTES

This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts.

This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.

DEFINED APPROACH TESTING PROCEDURES

3.4.1.a Examine documented policies and procedures for masking the display of PANs to verify:

- A list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN) is documented, together with a legitimate business need for each role to have such access.
- PAN is masked when displayed such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.
- All roles not specifically authorized to see the full PAN must only see masked PANs.

3.4.1.b Examine system configurations to verify that full PAN is only displayed for roles with a documented business need, and that PAN is masked for all other requests.

3.4.1.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displayed, and that only those with a legitimate business need are able to see more than the BIN and/or last four digits of the PAN.

GUIDANCE

Purpose

The display of full PAN on computer screens, payment card receipts, paper reports, etc. can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that the full PAN is displayed only for those with a legitimate business need minimizes the risk of unauthorized persons gaining access to PAN data.

Good Practice

Applying access controls according to defined roles is one way to limit access to viewing full PAN to only those individuals with a defined business need.

The masking approach should always display only the number of digits needed to perform a specific business function. For example, if only the last four digits are needed to perform a business function, PAN should be masked to only show the last four digits. As another example, if a function needs to view to the bank identification number (BIN) for routing purposes, unmask only the BIN digits for that function.

Definitions

Masking is not synonymous with truncation and these terms cannot be used interchangeably. Masking refers to the concealment of certain digits during display or printing, even when the entire PAN is stored on a system. This is different from truncation,

in which the truncated digits are removed and cannot be retrieved within the system. Masked PAN could be “unmasked”, but there is no "un-truncation" without recreating the PAN from another source.

Examples

Further Information

For more information about masking and truncation, see PCI SSC’s FAQs on these topics.

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.

CUSTOMIZED APPROACH OBJECTIVE

PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.

APPLICABILITY NOTES

Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.4.2.a Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following:

- Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN.
- A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.

3.4.2.b Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.

3.4.2.c Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.

GUIDANCE

Purpose

Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently.

Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN.

Good Practice

Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.

Definitions

A virtual desktop is an example of a remote-access technology.

Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.

Examples

Further Information

Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES 3.5

3.5 Primary account number (PAN) is secured wherever it is stored.

DEFINED APPROACH REQUIREMENTS

3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches:

- One-way hashes based on strong cryptography of the entire PAN.
- Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.
- Index tokens.
- Strong cryptography with associated key-management processes and procedures.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext PAN cannot be read from storage media.

APPLICABILITY NOTES

It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN.

This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.

DEFINED APPROACH TESTING PROCEDURES

3.5.1.a Examine documentation about the system used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the methods specified in this requirement.

3.5.1.b Examine data repositories and audit logs, including payment application logs, to verify the PAN is rendered unreadable using any of the methods specified in this requirement.

3.5.1.c If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

GUIDANCE

Purpose

The removal of cleartext stored PAN is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control.

Secondary independent control systems (for example governing access to, and use of, cryptography and decryption keys) prevent the failure of a primary access control system leading to a breach of confidentiality of stored PAN. If hashing is used to remove stored cleartext PAN, by correlating hashed and truncated versions of a given PAN, a malicious individual can easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable.

Good Practice

Definitions

Examples

Further Information

For information about truncation formats and truncation in general, see PCI SSC's FAQs on the topic.

Sources for information about index tokens include:

- PCI SSC's Tokenization Product Security Guidelines (*https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf*)
- *ANSI X9.119-2-2017: Retail Financial Services - Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.5.1.1.a Examine documentation about the hashing method used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (as applicable) to verify that the hashing method results in keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures.

3.5.1.1.b Examine documentation about the key management procedures and processes associated with the keyed cryptographic hashes to verify keys are managed in accordance with Requirements 3.6 and 3.7.

3.5.1.1.c Examine data repositories to verify the PAN is rendered unreadable.

3.5.1.1.d Examine audit logs, including payment application logs, to verify the PAN is rendered unreadable.

GUIDANCE

Purpose

The removal of cleartext stored PAN is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity’s primary access control.

Secondary independent control systems (for example governing access to, and use of, cryptography and decryption keys) prevent the failure of a primary access control system leading to a breach of confidentiality of stored PAN.

Good Practice

A hashing function that incorporates a randomly generated secret key provides brute force attack resistance and secret authentication integrity.

Definitions

Examples

Further Information

Appropriate keyed cryptographic hashing algorithms include but are not limited to: HMAC, CMAC, and GMAC, with an effective cryptographic strength of at least 128-bits (*NIST SP 800-131Ar2*).

Refer to the following for more information about HMAC, CMAC, and GMAC, respectively: *NIST SP 800-107r1, NIST SP 800-38B, and NIST SP 800-38D).*

See *NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms §5.3.*

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:

- On removable electronic media OR
- If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices.

Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies.

Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.5.1.2.a Examine encryption processes to verify that, if disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows:

- On removable electronic media, OR
- If used for non-removable electronic media, examine encryption processes used to verify that PAN is also rendered unreadable via another method that meets Requirement 3.5.1.

3.5.1.2.b Examine configurations and/or vendor documentation and observe encryption processes to verify the system is configured according to vendor documentation the result is that the disk or the partition is rendered unreadable.

GUIDANCE

Purpose

Disk-level and partition-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. For this reason, disk-level encryption is not appropriate to protect stored PAN on computers, laptops, servers, storage arrays, or any other system that provides transparent decryption upon user authentication.

Good Practice

Definitions

Examples

Further Information

Where available, following vendors' hardening and industry best practice guidelines can assist in securing PAN on these devices.

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows:

- Logical access is managed separately and independently of native operating system authentication and access control mechanisms.
- Decryption keys are not associated with user accounts.
- Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

CUSTOMIZED APPROACH OBJECTIVE

Disk encryption implementations are configured to require independent authentication and logical access controls for decryption

APPLICABILITY NOTES

Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.

DEFINED APPROACH TESTING PROCEDURES

3.5.1.3.a If disk-level or partition-level encryption is used to render PAN unreadable, examine the system configuration and observe the authentication process to verify that logical access is implemented in accordance with all elements specified in this requirement.

3.5.1.3.b Examine files containing authentication factors (passwords, passphrases, or cryptographic keys) and interview personnel to verify that authentication factors that allow access to unencrypted data are stored securely and are independent from the native operating system's authentication and access control methods.

GUIDANCE

Purpose

Disk-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and perform the appropriate cryptographic transformations without any special action by the user other than supplying a password or passphrase at system start-up or at the beginning of a session. This provides no protection from a malicious individual that has already managed to gain access to a valid user account.

Good Practice

Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is best limited only to removable electronic media storage devices.

Definitions

Examples

Further Information

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES 3.6

3.6 Cryptographic keys used to protect stored account data are secured.

DEFINED APPROACH REQUIREMENTS

3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include:

- Access to keys is restricted to the fewest number of custodians necessary.
- Key-encrypting keys are at least as strong as the data-encrypting keys they protect.
- Key-encrypting keys are stored separately from data-encrypting keys.
- Keys are stored securely in the fewest possible locations and forms.

CUSTOMIZED APPROACH OBJECTIVE

Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.

APPLICABILITY NOTES

This requirement applies to keys used to encrypt stored account data and to key-encrypting keys used to protect data-encrypting keys.

The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.

DEFINED APPROACH TESTING PROCEDURES

3.6.1 Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.

GUIDANCE

Purpose

Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data.

Good Practice

Having a centralized key management system based on industry standards is recommended for managing cryptographic keys.

Definitions

Examples

Further Information

The entity's key management procedures will benefit through alignment with industry requirements, Sources for information on cryptographic key management life cycles include:

- *ISO 11568-1 Banking — Key management (retail) — Part 1: Principles (specifically Chapter 10 and the referenced Parts 2 & 4)*
- *NIST SP 800-57 Part 1 Revision 5—Recommendation for Key Management, Part 1: General.*

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.6.1.1 Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes:

- Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date.
- Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.

- Description of the key usage for each key.
- Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.

CUSTOMIZED APPROACH OBJECTIVE

Accurate details of the cryptographic architecture are maintained and available.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement will be shared between the cloud provider and the cloud customer.

The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys in production and test is prevented) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

3.6.1.1 Additional testing procedure for service provider assessments only: Interview responsible personnel and examine documentation to verify that a document exists to describe the cryptographic architecture that includes all elements specified in this requirement.

GUIDANCE

Purpose

Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect stored account data, as well as the devices that generate, use, and protect the keys. This allows an entity to keep pace with evolving threats to its architecture and plan for updates as the assurance level provided by different algorithms and key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices and identify unauthorized additions to its cryptographic architecture.

The use of the same cryptographic keys in both production and test environments introduces a risk of exposing the key if the test environment is not at the same security level

as the production environment.

Good Practice

Having an automated reporting mechanism can assist with maintenance of the cryptographic attributes.

Definitions

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.
- Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.
- As at least two full-length key components or key shares, in accordance with an industry-accepted method.

CUSTOMIZED APPROACH OBJECTIVE

Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access.

APPLICABILITY NOTES

It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following:

- Using an approved random number generator and within an SCD, OR
- According to ISO 19592 or equivalent industry standard for generation of secret key shares.

DEFINED APPROACH TESTING PROCEDURES

3.6.1.2.a Examine documented procedures to verify it is defined that cryptographic keys used to encrypt/decrypt stored account data must exist only in one (or more) of the forms specified in this requirement. 3.6.1.2.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt stored account data exist in one (or more) of the forms specified in this requirement. 3.6.1.2.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:

- Key-encrypting keys are at least as strong as the data-encrypting keys they protect.
- Key-encrypting keys are stored separately from data-encrypting keys.

GUIDANCE

Purpose

Storing cryptographic keys securely prevents unauthorized or unnecessary access that could result in the exposure of stored account data. Storing keys separately means they are stored such that if the location of one key is compromised, the second key is not also compromised.

Good Practice

Where data-encrypting keys are stored in an HSM, the HSM interaction channel should be protected to prevent interception of encryption or decryption operations.

Definitions

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.

CUSTOMIZED APPROACH OBJECTIVE

Access to cleartext cryptographic key components is restricted to necessary personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.6.1.3 Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.

GUIDANCE

Purpose

Restricting the number of people who have access to cleartext cryptographic key components reduces the risk of stored account data being retrieved or rendered visible by unauthorized parties.

Good Practice

Only personnel with defined key custodian responsibilities (creating, altering, rotating, distributing, or otherwise maintaining encryption keys) should be granted access to key components. Ideally this will be a very small number of people.

Definitions

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.6.1.4 Cryptographic keys are stored in the fewest possible locations.

CUSTOMIZED APPROACH OBJECTIVE

Cryptographic keys are retained only where necessary.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.6.1.4 Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.

GUIDANCE

Purpose

Storing any cryptographic keys in the fewest locations helps an organization track and monitor all key locations and minimizes the potential for keys to be exposed to unauthorized parties.

Good Practice

Definitions

Examples

Further Information

sections 3 | top

REQUIREMENTS and TESTING PROCEDURES 3.7

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

DEFINED APPROACH REQUIREMENTS

3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.

CUSTOMIZED APPROACH OBJECTIVE

Strong cryptographic keys are generated.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.7.1.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define generation of strong cryptographic keys.

3.7.1.b Observe the method for generating keys to verify that strong keys are generated.

GUIDANCE

Purpose

Use of strong cryptographic keys significantly increases the level of security of encrypted account data.

Good Practice

Definitions

Examples

Further Information

See the sources referenced at "Cryptographic Key Generation in Appendix G.

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.

CUSTOMIZED APPROACH OBJECTIVE

Cryptographic keys are secured during distribution.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.7.2.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys. 3.7.2.b Observe the method for distributing keys to verify that keys are distributed securely.

GUIDANCE

Purpose

Secure distribution or conveyance of secret or private cryptographic keys means that keys are distributed only to authorized custodians, as identified in Requirement 3.6.1.2, and are never distributed insecurely.

Good Practice

Definitions

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.

CUSTOMIZED APPROACH OBJECTIVE

Cryptographic keys are secured when stored.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.7.3.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure storage of cryptographic keys.

3.7.3.b Observe the method for storing keys to verify that keys are stored securely.

GUIDANCE

Purpose

Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of account data.

Good Practice

Data encryption keys can be protected by encrypting them with a key-encrypting key.

Keys can be stored in a Hardware Security Module (HSM).

Secret or private keys that can decrypt data should never be present in source code.

Definitions

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:

- A defined cryptoperiod for each key type in use.
- A process for key changes at the end of the defined cryptoperiod.

CUSTOMIZED APPROACH OBJECTIVE

Cryptographic keys are not used beyond their defined cryptoperiod.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.7.4.a Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define changes to cryptographic keys that have reached the end of their cryptoperiod and include all elements specified in this requirement.

3.7.4.b Interview personnel, examine documentation, and observe key storage locations to verify that keys are changed at the end of the defined cryptoperiod(s).

GUIDANCE

Purpose

Changing encryption keys when they reach the end of their cryptoperiod is imperative to minimize the risk of someone obtaining the encryption keys and using them to decrypt data.

Good Practice

Definitions

A cryptoperiod is the time span during which a cryptographic key can be used for its defined purpose. Cryptoperiods are often defined in terms of the period for which the key is active

and/or the amount of cipher-text that has been produced by the key. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted.

Examples

Further Information

NIST SP 800-57 Part 1, Revision 5, Section 5.3 Cryptoperiods - provides guidance for establishing the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect. See Table 1 of *SP 800-57* Part 1 for suggested cryptoperiods for different key types.

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:

- The key has reached the end of its defined cryptoperiod.
- The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known.
- The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.

CUSTOMIZED APPROACH OBJECTIVE

Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.

APPLICABILITY NOTES

Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.

DEFINED APPROACH TESTING PROCEDURES

3.7.5.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define retirement, replacement, or destruction of keys in accordance with all elements specified in this requirement.

3.7.5.b Interview personnel to verify that processes are implemented in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Keys that are no longer required, keys with weakened integrity, and keys that are known or suspected to be compromised, should be archived, revoked, and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived encrypted data), they should be strongly protected.

Good Practice

Archived cryptographic keys should be used only for decryption/verification purposes. The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan per Requirement 12.10.1.

Definitions

Examples

Further Information

Industry best practices for archiving retired keys are outlined in *NIST SP 800-57 Part 1, Revision 5, Section 8.3.1*, and includes maintaining the archive with a trusted third party and storing archived key information separately from operational data.

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person

APPLICABILITY NOTES

This control is applicable for manual key-management operations or where key management is not controlled by the encryption product. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following:

- Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device, OR
- According to ISO 19592 or equivalent industry standard for generation of secret key shares.

DEFINED APPROACH TESTING PROCEDURES

3.7.6.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define using split knowledge and dual control.

3.7.6.b Interview personnel and/or observe processes to verify that manual cleartext keys are managed with split knowledge and dual control.

GUIDANCE

Purpose

Split knowledge and dual control of keys are used to eliminate the possibility of a single person having access to the whole key and therefore being able to gain unauthorized access to the data.

Good Practice

Where key components or key shares are used, procedures should ensure that no single custodian ever has access to sufficient key components or shares to reconstruct the cryptographic key. For example, in an m-of-n scheme (for example, Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian should not

then be assigned component B or C, as this would give the custodian knowledge of two components and the ability to recreate the key.

Definitions

Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of other components or of the original cryptographic key.

Dual control requires two or more people to authenticate the use of a cryptographic key or perform a key-management function. No single person can access or use the authentication factor (for example, the password, PIN, or key) of another.

Examples

Key-management operations that might be performed manually include, but are not limited to, key generation, transmission, loading, storage, and destruction.

Further Information

Industry standards for managing key components include: •* NIST SP 800-57* Part 2, Revision 1 -- Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations [4.6 Keying Material Distribution]

- *ISO 11568-2 Banking — Key management (retail) — Part 2*: Symmetric ciphers, their key management and life cycle [4.7.2.3 Key components and 4.9.3 Key components]
- *European Payments Council EPC342-08 Guidelines on Cryptographic Algorithms Usage and Key Management* [especially 4.1.4 Key installation].

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.

CUSTOMIZED APPROACH OBJECTIVE

Cryptographic keys cannot be substituted by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.7.7.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define prevention of unauthorized substitution of cryptographic keys.

3.7.7.b Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.

GUIDANCE

Purpose

If an attacker is able to substitute an entity's key with a key the attacker knows, the attacker will be able to decrypt all data encrypted with that key.

Good Practice

The encryption solution should not allow for or accept substitution of keys from unauthorized sources or unexpected processes.

Controls should include ensuring that individuals with access to key components or shares do not have access to other components or shares that form the necessary threshold to derive the key.

Definitions

Examples

Further Information

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

CUSTOMIZED APPROACH OBJECTIVE

Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

3.7.8.a Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define acknowledgments for key custodians in accordance with all elements specified in this requirement.

3.7.8.b Examine documentation or other evidence showing that key custodians have provided acknowledgments in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities. An annual reaffirmation can help remind key custodians of their responsibilities.

Good Practice

Definitions

Examples

Further Information

Industry guidance for key custodians and their roles and responsibilities includes:

- *NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems* [5. Roles and Responsibilities (especially) for Key Custodians]
- *ISO 11568-1 Banking -- Key management (retail) -- Part 1*: Principles [5 Principles of key management (especially b)]

sections 3 | top

DEFINED APPROACH REQUIREMENTS

3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider’s customers.

CUSTOMIZED APPROACH OBJECTIVE

Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

3.7.9 Additional testing procedure for service provider assessments only: If the service provider shares cryptographic keys with its customers for transmission or storage of account data, examine the documentation that the service provider provides to its customers to verify it includes guidance on how to securely transmit, store, and update customers' keys in accordance with all elements specified in Requirements 3.7.1 through 3.7.8 above.

GUIDANCE

Purpose

Providing guidance to customers on how to securely transmit, store, and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities.

Good Practice

Definitions

Examples

Further Information

Numerous industry standards for key management are cited above in the Guidance for Requirements 3.7.1-3.7.8.

sections 3 | top

PRINCIPLE PCI DSS REQUIREMENT: Protect Account Data

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

OVERVIEW

The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and non-repudiation.

To protect against compromise, PAN must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to cardholder data environments (CDE). Any transmissions of cardholder data over an entity's internal network(s) will naturally bring that network into scope for PCI DSS since that network stores, processes, or transmits cardholder data. Any such networks must be evaluated and assessed against applicable PCI DSS requirements.

Requirement 4 applies to transmissions of PAN unless specifically called out in an individual requirement.

PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is recommended.

Refer to Appendix G for definitions of "strong cryptography" and other PCI DSS terms.

SECTIONS 4

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

4.2 PAN is protected with strong cryptography during transmission.

requirement 4 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 4.1

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

DEFINED APPROACH REQUIREMENTS

4.1.1 All security policies and operational procedures that are identified in Requirement 4 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

4.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 4 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 4.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 4. While it is important to define the specific policies or procedures called out in Requirement 4, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives. Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.

Examples

Further Information

sections 4 | top

DEFINED APPROACH REQUIREMENTS

4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

4.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 4 are documented and assigned.

4.1.2.b Interview personnel with responsibility for performing activities in Requirement 4 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 4 | top

REQUIREMENTS and TESTING PROCEDURES 4.2

4.2 PAN is protected with strong cryptography during transmission.

DEFINED APPROACH REQUIREMENTS

are implemented as follows to safeguard PAN during transmission over open, public networks:

- Only trusted keys and certificates are accepted.
- Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.*
- The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.
- The encryption strength is appropriate for the encryption methodology in use.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.

APPLICABILITY NOTES

There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data.

A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. Note that self-signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable.

The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

4.2.1.a Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement.

4.2.1.b Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement.

4.2.1.c Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks.

4.2.1.d Examine system configurations to verify that keys and/or certificates that cannot be verified as trusted are rejected.

GUIDANCE

Purpose

Sensitive information must be encrypted during transmission over public networks because it is easy and common for a malicious individual to intercept and/or divert data while in transit.

Good Practice

The network and data-flow diagrams defined in Requirement 1 are useful resources for identifying all connection points where account data is transmitted or received over open,

public networks.

While not required, it is considered a good practice for entities to also encrypt PAN over their internal networks, and for entities to establish any new network implementations with encrypted communications.

PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is strongly recommended. If encrypted at the data level, the cryptographic keys used for protecting the data can be managed in accordance with Requirements 3.6 and 3.7. If the data is encrypted at the session level, designated key custodians should be assigned responsibility for managing transmission keys and certificates.

Some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain access to the cleartext data. It is critical that entities maintain awareness of industry-defined deprecation dates for the cipher suites they are using and are prepared to migrate to newer versions or protocols when older ones are no longer deemed secure.

Verifying that certificates are trusted helps ensure the integrity of the secure connection. To be considered trusted, a certificate should be issued from a trusted source, such as a trusted certificate authority (CA), and not be expired. Up-to-date Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used to validate certificates.

Techniques to validate certificates may include certificate and public key pinning, where the trusted certificate or a public key is pinned either during development or upon its first use. Entities can also confirm with developers or review source code to ensure that clients and servers reject connections if the certificate is bad.

For browser-based TLS certificates, certificate trust can often be verified by clicking on the lock icon that appears next to the address bar.

Definitions

Examples

Open, public networks include, but are not limited to:

- The Internet and
- Wireless technologies, including Wi-Fi, Bluetooth, cellular technologies, and satellite communications.

Further Information

Vendor recommendations and industry best practices can be consulted for information about the proper encryption strength specific to the encryption methodology in use. For more information about strong cryptography and secure protocols, see industry standards and best practices such as *NIST SP 800-52 and SP 800-57.* For more information about trusted keys and certificates, see *NIST Cybersecurity Practice Guide Special Publication 1800-16, Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.*

sections 4 | top

DEFINED APPROACH REQUIREMENTS

4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.

CUSTOMIZED APPROACH OBJECTIVE

All keys and certificates used to protect PAN during transmission are identified and confirmed as trusted.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

4.2.1.1.a Examine documented policies and procedures to verify processes are defined for the entity to maintain an inventory of its trusted keys and certificates.

4.2.1.1.b Examine the inventory of trusted keys and certificates to verify it is kept up to date.

GUIDANCE

Purpose

The inventory of trusted keys helps the entity keep track of the algorithms, protocols, key strength, key custodians, and key expiry dates. This enables the entity to respond quickly to vulnerabilities discovered in encryption software, certificates, and cryptographic algorithms.

Good Practice

For certificates, the inventory should include the issuing CA and certification expiration date.

Definitions

Examples

Further Information

sections 4 | top

DEFINED APPROACH REQUIREMENTS

4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext PAN cannot be read or intercepted from wireless network transmissions.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

4.2.1.2 Examine system configurations to verify that wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

GUIDANCE

Purpose

Since wireless networks do not require physical media to connect, it is important to establish controls limiting who can connect and what transmission protocols will be used. Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks.

Wireless networks present unique risks to an organization; therefore, they must be identified and protected according to industry requirements. Strong cryptography for authentication and transmission of PAN is required to prevent malicious users from gaining

access to the wireless network or utilizing wireless networks to access other internal networks or data.

Good Practice

Wireless networks should not permit fallback or downgrade to an insecure protocol or lower encryption strength that does not meet the intent of strong cryptography.

Definitions

Examples

Further Information

Review the vendor's specific documentation for more details on the choice of protocols, configurations, and settings related to cryptography.

sections 4 | top

DEFINED APPROACH REQUIREMENTS

4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.

APPLICABILITY NOTES

This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user messaging technologies.

There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.

DEFINED APPROACH TESTING PROCEDURES

4.2.2.a Examine documented policies and procedures to verify that processes are defined to secure PAN with strong cryptography whenever sent over end-user messaging technologies.

4.2.2.b Examine system configurations and vendor documentation to verify that PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.

GUIDANCE

Purpose

End-user messaging technologies typically can be easily intercepted by packet-sniffing during delivery across internal and public networks.

Good Practice

The use of end-user messaging technology to send PAN should only be considered where there is a defined business need.

Definitions

Examples

E-mail, instant messaging, SMS, and chat are examples of the type of end-user messaging technology that this requirement refers to.

Further Information

sections 4 | top

PRINCIPLE PCI DSS REQUIREMENT: Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

OVERVIEW

Malicious software (malware) is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner’s data, applications, or operating system.

Examples include viruses, worms, Trojans, spyware, ransomware, keyloggers, and rootkits, malicious code, scripts, and links.

Malware can enter the network during many business-approved activities, including employee e-mail (for example, via phishing) and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities.

Using anti-malware solutions that address all types of malware helps to protect systems from current and evolving malware threats. Refer to Appendix G for definitions of PCI DSS terms

SECTIONS 5

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

requirement 5 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 5.1

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

DEFINED APPROACH REQUIREMENTS

5.1.1 All security policies and operational procedures that are identified in Requirement 5 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 5 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 5.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 5. While it is important to define the specific policies or procedures called out in Requirement 5, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 5 are documented and assigned.

5.1.2.b Interview personnel with responsibility for performing activities in Requirement 5 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 5 | top

REQUIREMENTS and TESTING PROCEDURES 5.2

5.2 Malicious software (malware) is prevented, or detected and addressed.

DEFINED APPROACH REQUIREMENTS

5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.

CUSTOMIZED APPROACH OBJECTIVE

Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.2.1.a Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.

5.2.1.b For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.

GUIDANCE

Purpose

There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data.

Good Practice

It is beneficial for entities to be aware of "zero-day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior.

Definitions

System components known to be affected by malware have active malware exploits available in the real world (not only theoretical exploits).

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.2.2 The deployed anti-malware solution(s):

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

CUSTOMIZED APPROACH OBJECTIVE

Malware cannot execute or infect other system components.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.2.2 Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution:

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

GUIDANCE

Purpose

It is important to protect against all types and forms of malware to prevent unauthorized access.

Good Practice

Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning.

Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network.

Definitions

Examples

Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following:

- A documented list of all system components not at risk for malware.
- Identification and evaluation of evolving malware threats for those system components.
- Confirmation whether such system components continue to not require anti-malware protection.

CUSTOMIZED APPROACH OBJECTIVE

The entity maintains awareness of evolving malware threats to ensure that any systems not protected from malware are not at risk of infection.

APPLICABILITY NOTES

System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1.

DEFINED APPROACH TESTING PROCEDURES

5.2.3.a Examine documented policies and procedures to verify that a process is defined for periodic evaluations of any system components that are not at risk for malware that includes all elements specified in this requirement.

5.2.3.b Interview personnel to verify that the evaluations include all elements specified in this requirement.

5.2.3.c Examine the list of system components identified as not at risk of malware and compare to the system components without an anti-malware solution deployed per Requirement 5.2.1 to verify that the system components match for both requirements.

GUIDANCE

Purpose

Certain systems, at a given point in time, may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-malware forums to determine whether its systems might be coming under threat from new and evolving malware.

Good Practice

If an entity determines that a particular system is not susceptible to any malware, the determination should be supported by industry evidence, vendor resources, and best practices. The following steps can help entities during their periodic evaluations:

- Identification of all system types previously determined to not require malware protection.
- Review of industry vulnerability alerts and notices to determine if new threats exist for any identified system.
- A documented conclusion about whether the system types remain not susceptible to malware.
- A strategy to add malware protection for any system types for which malware protection has become necessary. Trends in malware should be included in the identification of new security vulnerabilities at Requirement 6.3.1, and methods to address new trends should be incorporated into the entity's configuration standards and protection mechanisms as needed.

Definitions

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

CUSTOMIZED APPROACH OBJECTIVE

Systems not known to be at risk from malware are re-evaluated at a frequency that addresses the entity's risk.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

5.2.3.1.a Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.

5.2.3.1.b Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.

GUIDANCE

Purpose

Entities determine the optimum period to undertake the evaluation based on criteria such as the complexity of each entity's environment and the number of types of systems that are required to be evaluated

Good Practice

Definitions

Examples

Further Information

sections 5 | top

REQUIREMENTS and TESTING PROCEDURES 5.3

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

DEFINED APPROACH REQUIREMENTS

5.3.1 The anti-malware solution(s) is kept current via automatic updates.

CUSTOMIZED APPROACH OBJECTIVE

Anti-malware mechanisms can detect and address the latest malware threats.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.3.1.a Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution is configured to perform automatic updates.

5.3.1.b Examine system components and logs, to verify that the anti-malware solution(s) and definitions are current and have been promptly deployed.

GUIDANCE

Purpose

For an anti-malware solution to remain effective, it needs to have the latest security updates, signatures, threat analysis engines, and any other malware protections on which the solution relies.

Having an automated update process avoids burdening end users with responsibility for manually installing updates and provides greater assurance that anti-malware protection mechanisms are updated as quickly as possible after an update is released.

Good Practice

Anti-malware mechanisms should be updated via a trusted source as soon as possible after an update is available. Using a trusted common source to distribute updates to end-user systems helps ensure the integrity and consistency of the solution architecture.

Updates may be automatically downloaded to a central location—for example, to allow for testing—prior to being deployed to individual system components.

Definitions

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.3.2 The anti-malware solution(s):

- Performs periodic scans and active or real-time scans. OR
- Performs continuous behavioral analysis of systems or processes.

CUSTOMIZED APPROACH OBJECTIVE

Malware cannot complete execution.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.3.2.a Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.

5.3.2.b Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.

5.3.2.c Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.

GUIDANCE

Purpose

Periodic scans can identify malware that is present, but currently inactive, within the environment. Some malware, such as zero-day malware, can enter an environment before the scan solution is capable of detecting it. Performing regular periodic scans or continuous behavioral analysis of systems or processes helps ensure that previously undetectable malware can be identified, removed, and investigated to determine how it gained access to the environment.

Good Practice

Using a combination of periodic scans (scheduled and on-demand) and active, real-time (on-access) scanning helps ensure that malware residing in both static and dynamic elements of the CDE is addressed. Users should also be able to run on-demand scans on their systems if suspicious activity is detected – this can be useful in the early detection of malware.

Scans should include the entire file system, including all disks, memory, and start-up files and boot records (at system restart) to detect all malware upon file execution, including any software that may be resident on a system but not currently active. Scan scope should include all systems and software in the CDE, including those that are often overlooked such as email servers, web browsers, and instant messaging software.

Definitions

Active, or real-time, scanning checks files for malware upon any attempt to open, close, rename, or otherwise interact with a file, preventing the malware from being activated.

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

CUSTOMIZED APPROACH OBJECTIVE

Scans by the malware solution are performed at a frequency that addresses the entity's risk.

APPLICABILITY NOTES

This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

5.3.2.1.a Examine the entity's targeted risk analysis for the frequency of periodic malware scans to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.

5.3.2.1.b Examine documented results of periodic malware scans and interview personnel to verify scans are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.

GUIDANCE

Purpose

Entities can determine the optimum period to undertake periodic scans based on their own assessment of the risks posed to their environments.

Good Practice

Definitions

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.3.3 For removable electronic media, the anti-malware solution(s):

- Performs automatic scans of when the media is inserted, connected, or logically mounted, OR
- Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.

CUSTOMIZED APPROACH OBJECTIVE

Malware cannot be introduced to system components via external removable media.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

5.3.3.a Examine anti-malware solution(s) configurations to verify that, for removable electronic media, the solution is configured to perform at least one of the elements specified in this requirement.

5.3.3.b Examine system components with removable electronic media connected to verify that the solution(s) is enabled in accordance with at least one of the elements as specified in this requirement.

5.3.3.c Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.

GUIDANCE

Purpose

Portable media devices are often overlooked as an entry method for malware. Attackers will often pre-load malware onto portable devices such as USB and flash drives; connecting an infected device to a computer then triggers the malware, introducing new threats within the environment.

Good Practice

Definitions

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.

CUSTOMIZED APPROACH OBJECTIVE

Historical records of anti-malware actions are immediately available and retained for at least 12 months.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

5.3.4 Examine anti-malware solution(s) configurations to verify logs are enabled and retained in accordance with Requirement 10.5.1.

GUIDANCE

Purpose

It is important to track the effectiveness of the anti-malware mechanisms—for example, by confirming that updates and scans are being performed as expected, and that malware is identified and addressed. Audit logs also allow an entity to determine how malware entered the environment and track its activity when inside the entity's network.

Good Practice

Definitions

Examples

Further Information

sections 5 | top

DEFINED APPROACH REQUIREMENTS

5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.

CUSTOMIZED APPROACH OBJECTIVE

Anti-malware mechanisms cannot be modified by unauthorized personnel.

APPLICABILITY NOTES

Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active.

DEFINED APPROACH TESTING PROCEDURES

5.3.5.a Examine anti-malware configurations, to verify that the anti-malware mechanisms cannot be disabled or altered by users.

5.3.5.b Interview responsible personnel and observe processes to verify that any requests to disable or alter anti-malware mechanisms are specifically documented and authorized by management on a case-by-case basis for a limited time period.

GUIDANCE

Purpose

It is important that defensive mechanisms are always running so that malware is detected in real time. Ad-hoc starting and stopping of anti-malware solutions could allow malware to propagate unchecked and undetected.

Good Practice

Where there is a legitimate need to temporarily disable a system's anti-malware protection —for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action should be understood and approved by an appropriate management representative. Any disabling or altering of anti-malware mechanisms, including on administrators' own devices, should be performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable anti-malware on their own computers, but there should be alerting mechanisms in place when such software is disabled and then follow up that occurs to ensure correct processes were followed.

Definitions

Examples

Additional security measures that may need to be implemented for the period during which anti-malware protection is not active include disconnecting the unprotected system from the Internet while the anti-malware protection is disabled and running a full scan once it is re-enabled.

Further Information

sections 5 | top

REQUIREMENTS and TESTING PROCEDURES x.y

5.4 Anti-phishing mechanisms protect users against phishing attacks.

DEFINED APPROACH REQUIREMENTS

5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.

CUSTOMIZED APPROACH OBJECTIVE

Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.

APPLICABILITY NOTES

This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as email servers) are brought into scope for PCI DSS.

The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS.

Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

5.4.1 Observe implemented processes and examine mechanisms to verify controls are in place to detect and protect personnel against phishing attacks.

GUIDANCE

Purpose

Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing.

Good Practice

When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and

Domain Keys Identified Mail (DKIM) will help stop phishers from spoofing the entity's domain and impersonating personnel.

The deployment of technologies for blocking phishing emails and malware before they reach personnel, such as link scrubbers and server-side anti-malware, can reduce incidents and decrease the time required by personnel to check and report phishing attacks. Additionally, training personnel to recognize and report phishing emails can allow similar emails to be identified and permit them to be removed before being opened.

It is recommended (but not required) that anti-phishing controls are applied across an entity's entire organization.

Definitions

Phishing is a form of social engineering and describes the different methods used by attackers to trick personnel into disclosing sensitive information, such as user account names and passwords, and account data. Attackers will typically disguise themselves and attempt to appear as a genuine or trusted source, directing personnel to send an email response, click on a web link, or enter data into a compromised website. Mechanisms that can detect and prevent phishing attempts are often included in anti-malware solutions.

Examples

Further Information

See the following for more information about phishing:

National Cyber Security Centre - Phishing Attacks: Defending your Organization.

US Cybersecurity & Infrastructure Security Agency - Report Phishing Sites.

sections 5 | top

PRINCIPLE PCI DSS REQUIREMENT: Maintain a Vulnerability Management Program

Requirement 6: Develop and Maintain Secure Systems and Software

OVERVIEW

Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques. Code repositories that store application code, system configurations, or other configuration data that can impact the security of account data or the CDE are in scope for PCI DSS assessments.

See Relationship between PCI DSS and PCI SSC Software Standards on page 7 for information about the use of PCI SSC-validated software and software vendors, and how use of PCI SSC's software standards may help with meeting controls in Requirement 6. Refer to Appendix G for definitions of PCI DSS terms.

Note: Requirement 6 applies to all system components, except for section 6.2 for developing software securely, which applies only to *bespoke* and *custom software* used on any system component included in or connected to the CDE.

SECTIONS 6

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

requirement 6 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 6.1

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

DEFINED APPROACH REQUIREMENTS

6.1.1 All security policies and operational procedures that are identified in Requirement 6 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 6 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 6.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 6. While it is important to define the specific policies or procedures called out in Requirement 6, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 6 are documented and assigned.

6.1.2.b Interview personnel responsible for performing activities in Requirement 6 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, systems will not be securely maintained, and their security level will be reduced.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 6 | top

REQUIREMENTS and TESTING PROCEDURES 6.2

6.2 Bespoke and custom software are developed securely.

DEFINED APPROACH REQUIREMENTS

6.2.1 Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- In accordance with PCI DSS (for example, secure authentication and logging).
- Incorporating consideration of information security issues during each stage of the software development lifecycle.

CUSTOMIZED APPROACH OBJECTIVE

Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.

APPLICABILITY NOTES

This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.

DEFINED APPROACH TESTING PROCEDURES

6.2.1 Examine documented software development procedures to verify that processes are defined that include all elements specified in this requirement.

GUIDANCE

Purpose

Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment.

Good Practice

Understanding how sensitive data is handled by the application—including when stored, transmitted, and in memory—can help identify where data needs to be protected.

PCI DSS requirements must be considered when developing software to meet those requirements by design, rather than trying to retrofit the software later.

Definitions

Examples

Secure software lifecycle management methodologies and frameworks include PCI Software Security Framework, BSIMM, OPENSAMM, and works from NIST, ISO, and SAFECode.

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

CUSTOMIZED APPROACH OBJECTIVE

Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.2.2.a Examine software development procedures to verify that processes are defined for training of software development personnel developing bespoke and custom software that includes all elements specified in this requirement.

6.2.2.b Examine training records and interview personnel to verify that software development personnel working on bespoke and custom software received software security training that is relevant to their job function and development languages in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices.

Good Practice

Training for developers may be provided in-house or by third parties.

Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software.

As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.

Definitions

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:

- Code reviews ensure code is developed according to secure coding guidelines.
- Code reviews look for both existing and emerging software vulnerabilities.
- Appropriate corrections are implemented prior to release.

CUSTOMIZED APPROACH OBJECTIVE

Bespoke and custom software cannot be exploited via coding vulnerabilities.

APPLICABILITY NOTES

This requirement for code reviews applies to all bespoke and custom software (both internal and public-facing), as part of the system development lifecycle.

Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4.

Code reviews may be performed using either manual or automated processes, or a combination of both.

DEFINED APPROACH TESTING PROCEDURES

6.2.3.a Examine documented software development procedures and interview responsible personnel to verify that processes are defined that require all bespoke and custom software to be reviewed in accordance with all elements specified in this requirement.

6.2.3.b Examine evidence of changes to bespoke and custom software to verify that the code changes were reviewed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Security vulnerabilities in bespoke and custom software are commonly exploited by malicious individuals to gain access to a network and compromise account data.

Vulnerable code is far more difficult and expensive to address after it has been deployed or released into production environments. Requiring a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures.

Good Practice

The following items should be considered for inclusion in code reviews:

- Searching for undocumented features (implant tools, backdoors).
- Confirming that software securely uses external components' functions (libraries, frameworks, APIs, etc.). For example, if a third-party library providing cryptographic functions is used, verify that it was integrated securely.
- Checking for correct use of logging to prevent sensitive data from getting into logs.
- Analysis of insecure code structures that may contain potential vulnerabilities related to common software attacks identified in Requirements 6.2.5.
- Checking the application's behavior to detect logical vulnerabilities.

Definitions

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

CUSTOMIZED APPROACH OBJECTIVE

The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.

APPLICABILITY NOTES

Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel.

An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.

DEFINED APPROACH TESTING PROCEDURES

6.2.3.1.a If manual code reviews are performed for bespoke and custom software prior to release to production, examine documented software development procedures and interview responsible personnel to verify that processes are defined for manual code reviews to be conducted in accordance with all elements specified in this requirement.

6.2.3.1.b Examine evidence of changes to bespoke and custom software and interview personnel to verify that manual code reviews were conducted in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Having code reviewed by someone other than the original author, who is both experienced in code reviews and knowledgeable about secure coding practices, minimizes the possibility that code containing security or logic errors that could affect the security of cardholder data is released into a production environment. Requiring management approval that the code was reviewed limits the ability for the process to be bypassed.

Good Practice

Having a formal review methodology and review checklists has been found to improve the quality of the code review process.

Code review is a tiring process, and for this reason, it is most effective when reviewers only review small amounts of code at a time.

To maintain the effectiveness of code reviews, it is beneficial to monitor the general workload of reviewers and to have them review applications they are familiar with.

Code reviews may be performed using either manual or automated processes, or a combination of both.

Entitles that rely solely on manual code review should ensure that reviewers maintain their skills through regular training as new vulnerabilities are found, and new secure coding methods are recommended.

Definitions

Examples

Further Information

See the OWASP Code Review Guide.

DEFINED APPROACH REQUIREMENTS

6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
- Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

CUSTOMIZED APPROACH OBJECTIVE

Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.

APPLICABILITY NOTES

This applies to all software developed for or by the entity for the entity’s own use. This includes both bespoke and custom software. This does not apply to third-party software.

DEFINED APPROACH TESTING PROCEDURES

6.2.4 Examine documented procedures and interview responsible software development personnel to verify that software engineering techniques or other methods are defined and

in use by developers of bespoke and custom software to prevent or mitigate all common software attacks as specified in this requirement.

GUIDANCE

Purpose

Detecting or preventing common errors that result in vulnerable code as early as possible in the software development process lowers the probability that such errors make it through to production and lead to a compromise. Having formal engineering techniques and tools embedded in the development process will catch these errors early. This philosophy is sometimes called “shifting security left.”

Good Practice

For both bespoke and custom software, the entity must ensure that code is developed focusing on the prevention or mitigation of common software attacks, including:

- Attempts to exploit common coding vulnerabilities (bugs).
- Attempts to exploit software design flaws.
- Attempts to exploit implementation/configuration flaws.
- Enumeration attacks – automated attacks that are actively exploited in payments and abuse identification, authentication, or authorization mechanisms. See the PCI Perspectives blog article “Beware of Account Testing Attacks.”

Researching and documenting software engineering techniques or other methods helps to define how software developers prevent or mitigate various software attacks by features or countermeasures they build into software. This might include identification/authentication mechanisms, access control, input validation routines, etc. Developers should be familiar with different types of vulnerabilities and potential attacks and use measures to avoid potential attack vectors when developing code.

Definitions

Examples

Techniques include automated processes and practices that scan code early in the development cycle when code is checked in to confirm the vulnerabilities are not present.

Further Information

sections 6 | top

REQUIREMENTS and TESTING PROCEDURES 6.3

6.3 Security vulnerabilities are identified and addressed.

DEFINED APPROACH REQUIREMENTS

6.3.1 Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

CUSTOMIZED APPROACH OBJECTIVE

New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.

APPLICABILITY NOTES

This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.

DEFINED APPROACH TESTING PROCEDURES

6.3.1.a Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.

6.3.1.b Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

Good Practice

Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.

When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.

An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.

Definitions

Examples

Some organizations that issue alerts to advise entities about urgent vulnerabilities requiring immediate patches/updates are national Computer Emergency Readiness/Response Teams (CERTs) and vendors.

Criteria for ranking vulnerabilities may include criticality of a vulnerability identified in an alert from Forum of Incident Response and Security Teams (FIRST) or a CERT, consideration of the CVSS score, the classification by the vendor, and/or type of systems affected.

Further Information

Trustworthy sources for vulnerability information include vendor websites, industry newsgroups, mailing lists, etc. If software is developed in-house, the internal development team should also consider sources of information about new vulnerabilities that may affect

internally developed applications. Other methods to ensure new vulnerabilities are identified include solutions that automatically recognize and alert upon detection of unusual behavior. Processes should account for widely published exploits as well as “zero-day” attacks, which target previously unknown vulnerabilities.

For bespoke and custom software, the organization may obtain information about libraries, frameworks, compilers, programming languages, etc. from public trusted sources (for example, special resources and resources from component developers). The organization may also independently analyze third-party components and identify vulnerabilities.

For control over in-house developed software, the organization may receive such information from external sources. The organization can consider using a “bug bounty” program where it posts information (for example, on its website) so third parties can contact the organization with vulnerability information. External sources may include independent investigators or companies that report to the organization about identified vulnerabilities and may include sources such as the Common Vulnerability Scoring System (CVSS) or the OWASP Risk Rating Methodology.

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.

CUSTOMIZED APPROACH OBJECTIVE

Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

6.3.2.a Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into

bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.

6.3.2.b Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.

GUIDANCE

Purpose

Identifying and listing all the entity's bespoke and custom software, and any third-party software that is incorporated into the entity's bespoke and custom software enables the entity to manage vulnerabilities and patches.

Vulnerabilities in third-party components (including libraries, APIs, etc.) embedded in an entity's software also renders those applications vulnerable to attacks. Knowing which third-party components are used in the entity's software and monitoring the availability of security patches to address known vulnerabilities is critical to ensuring the security of the software.

Good Practice

An entity's inventory should cover all payment software components and dependencies, including supported execution platforms or environments, third-party libraries, services, and other required functionalities.

There are many different types of solutions that can help with managing software inventories, such as software composition analysis tools, application discovery tools, and mobile device management.

Definitions

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

CUSTOMIZED APPROACH OBJECTIVE

System components cannot be compromised via the exploitation of a known vulnerability.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.3.3.a Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.

6.3.3.b Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data.

Good Practice

Prioritizing security patches/updates for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released.

An entity's patching cadence should factor in any re-evaluation of vulnerabilities and subsequent changes in the criticality of a vulnerability per Requirement 6.3.1. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk could collectively pose a

high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.

Definitions

Examples

Further Information

sections 6 | top

REQUIREMENTS and TESTING PROCEDURES 6.4

6.4 Public-facing web applications are protected against attacks.

DEFINED APPROACH REQUIREMENTS

6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections

OR

- Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web-based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.

CUSTOMIZED APPROACH OBJECTIVE

Public-facing web applications are protected against malicious attacks.

APPLICABILITY NOTES

This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2. This requirement will be superseded by Requirement 6.4.2 after 31

March 2025 when Requirement 6.4.2 becomes effective.

DEFINED APPROACH TESTING PROCEDURES

6.4.1 For public-facing web applications, ensure that either one of the required methods is in place as follows:

- If manual or automated vulnerability security assessment tools or methods are in use, examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed in accordance with all elements of this requirement specific to the tool/method.

OR

- If an automated technical solution(s) is installed that continually detects and prevents web-based attacks, examine the system configuration settings and audit logs, and interview responsible personnel to verify that the automated technical solution(s) is installed in accordance with all elements of this requirement specific to the solution(s).

GUIDANCE

Purpose

Public-facing web applications are those that are available to the public (not only for internal use). These applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems.

Good Practice

Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities. Common assessment tools include specialized web scanners that perform automatic analysis of web application protection.

When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated.

Definitions

Examples

A web application firewall (WAF) installed in front of public-facing web applications to check all traffic is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4). WAFs filter and block non-essential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured.

Another example of an automated technical solution is Runtime Application Self-Protection (RASP) technologies. When implemented correctly, RASP solutions can detect and block anomalous behavior by the software during execution. While WAFs typically monitor the application perimeter, RASP solutions monitor and block behavior within the application.

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:

- Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.
- Actively running and up to date as applicable.
- Generating audit logs.
- Configured to either block web-based attacks or generate an alert that is immediately investigated.

CUSTOMIZED APPROACH OBJECTIVE

Public-facing web applications are protected in real time against malicious attacks.

APPLICABILITY NOTES

This new requirement will replace Requirement 6.4.1 once its effective date is reached.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

6.4.2 For public-facing web applications, examine the system configuration settings and audit logs, and interview responsible personnel to verify that an automated technical

solution that detects and prevents web-based attacks is in place in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems.

Good Practice

When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated. Such solutions may also be used to automate mitigation, for example rate-limiting controls, which can be implemented to mitigate against brute-force attacks and enumeration attacks.

Definitions

Examples

A web application firewall (WAF), which can be either on-premise or cloud-based, installed in front of public-facing web applications to check all traffic, is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4). WAFs filter and block non-essential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured.

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorized.
- A method is implemented to assure the integrity of each script.
- An inventory of all scripts is maintained with written justification as to why each is necessary.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.

APPLICABILITY NOTES

This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

6.4.3.a Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser, in accordance with all elements specified in this requirement.

6.4.3.b Interview responsible personnel and examine inventory records and system configurations to verify that all payment page scripts that are loaded and executed in the consumer's browser are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Scripts loaded and executed in the payment page can have their functionality altered without the entity's knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems).

Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that can read and exfiltrate cardholder data from the consumer browser.

Ensuring that the functionality of all such scripts is understood to be necessary for the operation of the payment page minimizes the number of scripts that could be tampered with.

Ensuring that scripts have been explicitly authorized reduces the probability of unnecessary scripts being added to the payment page without appropriate management approval.

Using techniques to prevent tampering with the script will minimize the probability of the script being modified to carry out unauthorized behavior, such as skimming the cardholder

data from the payment page.

Good Practice

Scripts may be authorized by manual or automated (e.g., workflow) processes. Where the payment page will be loaded into an inline frame (IFRAME), restricting the location that the payment page can be loaded from, using the parent page's Content Security Policy (CSP) can help prevent unauthorized content being substituted for the payment page.

Definitions

"Necessary" for this requirement means that the entity's review of each script justifies and confirms why it is needed for the functionality of the payment page to accept a payment transaction.

Examples

The integrity of scripts can be enforced by several different mechanisms including, but not limited to:

- Sub-resource integrity (SRI), which allows the consumer browser to validate that a script has not been tampered with.
- A CSP, which limits the locations the consumer browser can load a script from and transmit account data to.
- Proprietary script or tag-management systems, which can prevent malicious script execution.

Further Information

sections 6 | top

REQUIREMENTS and TESTING PROCEDURES 6.5

6.5 Changes to all system components are managed securely.

DEFINED APPROACH REQUIREMENTS

6.5.1 Changes to all system components in the production environment are made according to established procedures that include:

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.

- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

CUSTOMIZED APPROACH OBJECTIVE

All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.5.1.a Examine documented change control procedures to verify procedures are defined for changes to all system components in the production environment to include all elements specified in this requirement.

6.5.1.b Examine recent changes to system components and trace those changes back to related change control documentation. For each change examined, verify the change is implemented in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Change management procedures must be applied to all changes—including the addition, removal, or modification of any system component—in the production environment. It is important to document the reason for a change and the change description so that relevant parties understand and agree the change is needed. Likewise, documenting the impacts of the change allows all affected parties to plan appropriately for any processing changes.

Good Practice

Approval by authorized parties confirms that the change is legitimate and that the change is sanctioned by the organization. Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change.

Thorough testing by the entity confirms that the security of the environment is not reduced by implementing a change and that all existing security controls either remain in place or are replaced with equal or stronger security controls after the change. The specific testing to be performed will vary according to the type of change and system component(s) affected.

For each change, it is important to have documented procedures that address any failures and provide instructions on how to return to a secure state in case the change fails or adversely affects the security of an application or system. These procedures will allow the application or system to be restored to its previous secure state.

Definitions

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

CUSTOMIZED APPROACH OBJECTIVE

All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.

APPLICABILITY NOTES

These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2.

DEFINED APPROACH TESTING PROCEDURES

6.5.2 Examine documentation for significant changes, interview personnel, and observe the affected systems/networks to verify that the entity confirmed applicable PCI DSS requirements were in place on all new or changed systems and networks and that documentation was updated as applicable.

GUIDANCE

Purpose

Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope

environment, and that PCI DSS requirements continue to be met to secure the environment.

Good Practice

Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed.

Definitions

Examples

Applicable PCI DSS requirements that could be impacted include, but are not limited to:

- Network and data-flow diagrams are updated to reflect changes.
- Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled.
- Systems are protected with required controls—for example, file integrity monitoring (FIM), anti-malware, patches, and audit logging.
- Sensitive authentication data is not stored, and all account data storage is documented and incorporated into data retention policy and procedures.
- New systems are included in the quarterly vulnerability scanning process.
- Systems are scanned for internal and external vulnerabilities after significant changes per Requirements 11.3.1.3 and 11.3.2.1.

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.

CUSTOMIZED APPROACH OBJECTIVE

Pre-production environments cannot introduce risks and vulnerabilities into production environments.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.5.3.a Examine policies and procedures to verify that processes are defined for separating the pre-production environment from the production environment via access controls that enforce the separation.

6.5.3.b Examine network documentation and configurations of network security controls to verify that the pre-production environment is separate from the production environment(s).

6.5.3.c Examine access control settings to verify that access controls are in place to enforce separation between the pre-production and production environment(s).

GUIDANCE

Purpose

Due to the constantly changing state of pre-production environments, they are often less secure than the production environment.

Good Practice

Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications.

Definitions

Pre-production environments include development, testing, user acceptance testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre-production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.

CUSTOMIZED APPROACH OBJECTIVE

Job roles and accountability that differentiate between pre-production and production activities are defined and managed to minimize the risk of unauthorized, unintentional, or inappropriate actions.

APPLICABILITY NOTES

In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.

DEFINED APPROACH TESTING PROCEDURES

6.5.4.a Examine policies and procedures to verify that processes are defined for separating roles and functions to provide accountability such that only reviewed and approved changes are deployed.

6.5.4.b Observe processes and interview personnel to verify implemented controls separate roles and functions and provide accountability such that only reviewed and approved changes are deployed.

GUIDANCE

Purpose

The goal of separating roles and functions between production and pre-production environments is to reduce the number of personnel with access to the production environment and account data and thereby minimize risk of unauthorized, unintentional, or inappropriate access to data and system components and help ensure that access is limited to those individuals with a business need for such access.

The intent of this control is to separate critical activities to provide oversight and review to catch errors and minimize the chances of fraud or theft (since two people would need to collude in order to hide an activity).

Separating roles and functions, also referred to as separation or segregation of duties, is a key internal control concept to protect an entity’s assets.

Good Practice

Definitions

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.

CUSTOMIZED APPROACH OBJECTIVE

Live PANs cannot be present in pre-production environments outside the CDE.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.5.5.a Examine policies and procedures to verify that processes are defined for not using live PANs in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.

6.5.5.b Observe testing processes and interview personnel to verify procedures are in place to ensure live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.

6.5.5.c Examine pre-production test data to verify live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.

GUIDANCE

Purpose

Use of live PANs outside of protected CDEs provides malicious individuals with the opportunity to gain unauthorized access to cardholder data.

Good Practice

Entities can minimize their storage of live PANs by only storing them in pre-production when strictly necessary for a specific and defined testing purpose and securely deleting that data after use.

If an entity requires PANs specifically designed for test purposes, these can be obtained from acquirers.

Definitions

Live PANs refer to valid PANs (not test PANs) that have the potential to be used to conduct payment transactions. Additionally, when payment cards expire, the same PAN is often reused with a different expiry date. All PANs must be verified as being unable to conduct payment transactions before they are excluded from PCI DSS scope. It is the responsibility of the entity to confirm that PANs are not live.

Examples

Further Information

sections 6 | top

DEFINED APPROACH REQUIREMENTS

6.5.6 Test data and test accounts are removed from system components before the system goes into production.

CUSTOMIZED APPROACH OBJECTIVE

Test data and test accounts cannot exist in production environments.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

6.5.6.a Examine policies and procedures to verify that processes are defined for removal of test data and test accounts from system components before the system goes into production.

6.5.6.b Observe testing processes for both off-the-shelf software and in-house applications, and interview personnel to verify test data and test accounts are removed before a system goes into production.

6.5.6.c Examine data and accounts for recently installed or updated off-the-shelf software and in-house applications to verify there is no test data or test accounts on systems in production.

GUIDANCE

Purpose

This data may give away information about the functioning of an application or system and is an easy target for unauthorized individuals to exploit to gain access to systems. Possession of such information could facilitate compromise of the system and related account data.

Good Practice

Definitions

Examples

Further Information

sections 6 | top

PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

OVERVIEW

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Access” or “access rights” are created by rules that provide users access to systems, applications, and data, while “privileges” allow a user to perform a specific action or function in relation to that system, application, or data. For example, a user may have access rights to specific data, but whether they can only read that data, or can also change or delete the data is determined by the user’s assigned privileges.

“Need to know” refers to providing access to only the least amount of data needed to perform a job.

“Least privileges” refers to providing only the minimum level of privileges needed to perform a job.

These requirements apply to user accounts and access for employees, contractors, consultants, and internal and external vendors and other third parties (for example, for providing support or maintenance services). Certain requirements also apply to application and system accounts used by the entity (also called “service accounts”).

These requirements do not apply to consumers (cardholders).

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 7

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

7.2 Access to system components and data is appropriately defined and assigned.

7.3 Access to system components and data is managed via an access control system(s).

requirement 7 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 7.1

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.

DEFINED APPROACH REQUIREMENTS

7.1.1 All security policies and operational procedures that are identified in Requirement 7 are:

- Documented.
- Kept up to date.

- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 7 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 7.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 7. While it is important to define the specific policies or procedures called out in Requirement 7, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 7 are documented and assigned.

7.1.2.b Interview personnel with responsibility for performing activities in Requirement 7 to verify that roles and responsibilities are assigned as and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 7 | top

REQUIREMENTS and TESTING PROCEDURES 7.2

7.2 Access to system components and data is appropriately defined and assigned.

DEFINED APPROACH REQUIREMENTS

7.2.1 An access control model is defined and includes granting access as follows:

- Appropriate access depending on the entity's business and access needs.
- Access to system components and data resources that is based on users' job classification and functions.
- The least privileges required (for example, user, administrator) to perform a job function.

CUSTOMIZED APPROACH OBJECTIVE

Access requirements are established according to job functions following least-privilege and need-to-know principles.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.2.1.a Examine documented policies and procedures and interview personnel to verify the access control model is defined in accordance with all elements specified in this requirement.

7.2.1.b Examine access control model settings and verify that access needs are appropriately defined in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Defining an access control model that is appropriate for the entity's technology and access control philosophy supports a consistent and uniform way of allocating access and reduces the possibility of errors such as the granting of excessive rights.

Good Practice

A factor to consider when defining access needs is the separation of duties principle. This principle is intended to prevent fraud and misuse or theft of resources. For example, 1) dividing mission-critical functions and information system support functions among different individuals and/or functions, 2) establishing roles such that information system support activities are performed by different functions/individuals (for example, system management, programming, configuration management, quality assurance and testing, and network security), and 3) ensuring security personnel administering access control functions do not also administer audit functions.

In environments where one individual performs multiple functions, such as administration and security operations, duties may be assigned so that no single individual has end-to-end control of a process without an independent checkpoint. For example, responsibility for configuration and responsibility for approving changes could be assigned to separate individuals.

Definitions

Key elements of an access control model include:

- Resources to be protected (the systems/devices/data to which access is needed),
- Job functions that need access to the resource (for example, system administrator, call-center personnel, store clerk), and
- Which activities each job function needs to perform (for example, read/write or query). Once job functions, resources, and activities per job functions are defined, individuals can be granted access accordingly.

Examples

Access control models that entities can consider include role-based access control (RBAC) and attribute-based access control (ABAC). The access control model used by a given entity depends on their business and access needs.

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.2.2 Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.

CUSTOMIZED APPROACH OBJECTIVE

Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.

APPLICABILITY NOTES

7.2.2.a Examine policies and procedures to verify they cover assigning access to users in accordance with all elements specified in this requirement.

7.2.2.b Examine user access settings, including for privileged users, and interview responsible management personnel to verify that privileges assigned are in accordance with all elements specified in this requirement.

7.2.2.c Interview personnel responsible for assigning access to verify that privileged user access is assigned in accordance with all elements specified in this requirement.

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.

Good Practice

Access rights are granted to a user by assignment to one or several functions. Assess is assigned depending on the specific user functions and with the minimum scope required for the job. When assigning privileged access, it is important to assign individuals only the privileges they need to perform their job (the “least privileges”). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator.

Once needs are defined for user functions (per PCI DSS requirement 7.2.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.

Entities may wish to consider use of Privileged Access Management (PAM), which is a method to grant access to privileged accounts only when those privileges are required,

immediately revoking that access once they are no longer needed.

Definitions

Examples

Further Information

sections 7 | top

REQUIREMENTS and TESTING PROCEDURES x.y

DEFINED APPROACH REQUIREMENTS

7.2.3 Required privileges are approved by authorized personnel.

CUSTOMIZED APPROACH OBJECTIVE

Access privileges cannot be granted to users without appropriate, documented authorization.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.2.3.a Examine policies and procedures to verify they define processes for approval of all privileges by authorized personnel.

7.2.3.b Examine user IDs and assigned privileges, and compare with documented approvals to verify that:

- Documented approval exists for the assigned privileges.
- The approval was by authorized personnel.
- Specified privileges match the roles assigned to the individual.

GUIDANCE

Purpose

Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.

Good Practice

Definitions

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:

- At least once every six months.
- To ensure user accounts and access remain appropriate based on job function.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

CUSTOMIZED APPROACH OBJECTIVE

Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.

APPLICABILITY NOTES

This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

7.2.4.a Examine policies and procedures to verify they define processes to review all user accounts and related access privileges, including third-party/vendor accounts, in accordance with all elements specified in this requirement.

7.2.4.b Interview responsible personnel and examine documented results of periodic reviews of user accounts to verify that all the results are in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Regular review of access rights helps to detect excessive access rights remaining after user job responsibilities change, system functions change, or other modifications. If excessive user rights are not revoked in due time, they may be used by malicious users for unauthorized access.

This review provides another opportunity to ensure that accounts for all terminated users have been removed (if any were missed at the time of termination), as well as to ensure that any third parties that no longer need access have had their access terminated.

Good Practice

When a user transfers into a new role or a new department, typically the privileges and access associated with their former role are no longer required. Continued access to privileges or functions that are no longer required may introduce the risk of misuse or errors. Therefore, when responsibilities change, processes that revalidate access help to ensure user access is appropriate for the user's new responsibilities.

Entities can consider implementing a regular, repeatable process for conducting reviews of access rights, and assigning "data owners" that are responsible for managing and monitoring access to data related to their job function and that also ensure user access remains current and appropriate. As an example, a direct manager could review team access monthly, while the senior manager reviews their groups' access quarterly, both making updates to access as needed. The intent of these best practices is to support and facilitate conducting the reviews at least once every 6 months.

Definitions

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.2.5 All application and system accounts and related access privileges are assigned and managed as follows:

- Based on the least privileges necessary for the operability of the system or application.
- Access is limited to the systems, applications, or processes that specifically require their use.

CUSTOMIZED APPROACH OBJECTIVE

Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

7.2.5.a Examine policies and procedures to verify they define processes to manage and assign application and system accounts and related access privileges in accordance with all elements specified in this requirement.

7.2.5.b Examine privileges associated with system and application accounts and interview responsible personnel to verify that application and system accounts and related access privileges are assigned and managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

It is important to establish the appropriate access level for application or system accounts. If such accounts are compromised, malicious users will receive the same access level as that granted to the application or system. Therefore, it is important to ensure limited access is granted to system and application accounts on the same basis as to user accounts.

Good Practice

Entities may want to consider establishing a baseline when setting up these application and system accounts including the following as applicable to the organization:

- Making sure that the account is not a member of a privileged group such as domain administrators, local administrators, or root.
- Restricting which computers the account can be used on.
- Restricting hours of use.
- Removing any additional settings like VPN access and remote access.

Definitions

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows:

- Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).
- The application/system access remains appropriate for the function being performed.
- Any inappropriate access is addressed.
- Management acknowledges that access remains appropriate.

CUSTOMIZED APPROACH OBJECTIVE

Application and system account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

7.2.5.1.a Examine policies and procedures to verify they define processes to review all application and system accounts and related access privileges in accordance with all elements specified in this requirement.

7.2.5.1.b Examine the entity's targeted risk analysis for the frequency of periodic reviews of application and system accounts and related access privileges to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.

7.2.5.1.c Interview responsible personnel and examine documented results of periodic reviews of system and application accounts and related privileges to verify that the reviews occur in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Regular review of access rights helps to detect excessive access rights remaining after system functions change, or other application or system modifications occur. If excessive rights are not removed when no longer needed, they may be used by malicious users for unauthorized access.

Good Practice

Definitions

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.2.6 All user access to query repositories of stored cardholder data is restricted as follows:

- Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.
- Only the responsible administrator(s) can directly access or query repositories of stored CHD.

CUSTOMIZED APPROACH OBJECTIVE

Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.

APPLICABILITY NOTES

This requirement applies to controls for user access to query repositories of stored cardholder data.

See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.

DEFINED APPROACH TESTING PROCEDURES

7.2.6.a Examine policies and procedures and interview personnel to verify processes are defined for granting user access to query repositories of stored cardholder data, in accordance with all elements specified in this requirement.

7.2.6.b Examine configuration settings for querying repositories of stored cardholder data to verify they are in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

The misuse of query access to repositories of cardholder data has been a regular cause of data breaches. Limiting such access to administrators reduces the risk of such access being abused by unauthorized users.

Good Practice

Typical user actions include moving, copying, and deleting data. Also consider the scope of privilege needed when granting access. For example, access can be granted to specific objects such as data elements, files, tables, indexes, views, and stored routines. Granting access to repositories of cardholder data should follow the same process as all other granted access, meaning that it is based on roles, with only the privileges assigned to each user that are needed to perform their job functions.

Definitions

“Programmatic methods” means granting access through means such as database stored procedures that allow users to perform controlled actions to data in a table, rather than via direct, unfiltered access to the data repository by end users (except for the responsible administrator(s), who need direct access to the database for their administrative duties).

Examples

Further Information

sections 7 | top

REQUIREMENTS and TESTING PROCEDURES 7.3

7.3 Access to system components and data is managed via an access control system(s).

DEFINED APPROACH REQUIREMENTS

7.3.1 An access control system(s) is in place that restricts access based on a user’s need to know and covers all system components.

CUSTOMIZED APPROACH OBJECTIVE

Access rights and privileges are managed via mechanisms intended for that purpose.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.3.1 Examine vendor documentation and system settings to verify that access is managed for each system component via an access control system(s) that restricts access based on a user's need to know and covers all system components.

GUIDANCE

Purpose

Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges.

Good Practice

Definitions

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.

CUSTOMIZED APPROACH OBJECTIVE

Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.3.2 Examine vendor documentation and system settings to verify that the access control system(s) is configured to enforce permissions assigned to individuals, applications, and

systems based on job classification and function.

GUIDANCE

Purpose

Restricting privileged access with an access control system reduces the opportunity for errors in the assignment of permissions to individuals, applications, and systems.

Good Practice

Definitions

Examples

Further Information

sections 7 | top

DEFINED APPROACH REQUIREMENTS

7.3.3 The access control system(s) is set to “deny all” by default.

CUSTOMIZED APPROACH OBJECTIVE

Access rights and privileges are prohibited unless expressly permitted.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

7.3.3 Examine vendor documentation and system settings to verify that the access control system(s) is set to “deny all” by default.

GUIDANCE

Purpose

A default setting of “deny all” ensures no one is granted access unless a rule is established specifically granting such access.

Good Practice

It is important to check the default configuration of access control systems because some are set by default to “allow all,” thereby permitting access unless/until a rule is written to specifically deny it.

Definitions

Examples

Further Information

sections 7 | top

PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures

Requirement 8: Identify Users and Authenticate Access to System Components

OVERVIEW

Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be.

Identification of an individual or process on a computer system is conducted by associating an identity with a person or process through an identifier, such as a user, system, or application ID. These IDs (also referred to as “accounts”) fundamentally establish the identity of an individual or process by assigning unique identification to each person or process to distinguish one user or process from another. When each user or process can be uniquely identified, it ensures there is accountability for actions performed by that identity. When such accountability is in place, actions taken can be traced to known and authorized users and processes.

The element used to prove or verify the identity is known as the authentication factor. Authentication factors are 1) something you know, such as a password or passphrase, 2) something you have, such as a token device or smart card, or 3) something you are, such as a biometric element.

The ID and the authentication factor together are considered authentication credentials and are used to gain access to the rights and privileges associated with a user, application, system, or service accounts.

These requirements for identity and authentication are based on industry-accepted security principles and best practices to support the payment ecosystem. NIST Special Publication 800-63, Digital Identity Guidelines provides additional information on acceptable frameworks for digital identity and authentication factors. It is important to note that the NIST Digital Identity Guidelines is intended for US Federal Agencies and should be viewed in its entirety. Many of the concepts and approaches defined in these guidelines are expected to work with each other and not as standalone parameters.

Note: Unless otherwise stated in the requirement, these requirements apply to all accounts on all system components, unless specifically called out in an individual requirement, including but not limited to: • Point-of-sale accounts • Accounts with administrative capabilities • System and application accounts • All accounts used to view or access cardholder data or to access systems with cardholder data.

This includes accounts used by employees, contractors, consultants, internal and external vendors, and other third parties (for example, for providing support or maintenance services).

Certain requirements are not intended to apply to user accounts that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). When items do not apply, they are noted directly within the specific requirement.

These requirements do not apply to accounts used by consumers (cardholders).

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 8

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account’s lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

requirement 8 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 8.1

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

DEFINED APPROACH REQUIREMENTS

8.1.1 All security policies and operational procedures that are identified in Requirement 8 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures that are identified in Requirement 8 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 8.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 8. While it is important to define the specific

policies or procedures called out in Requirement 8, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 8 are documented and assigned.

8.1.2.b Interview personnel with responsibility for performing activities in Requirement 8 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 8 | top

REQUIREMENTS and TESTING PROCEDURES 8.1

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

DEFINED APPROACH REQUIREMENTS

8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.

CUSTOMIZED APPROACH OBJECTIVE

All actions by all users are attributable to an individual.

APPLICABILITY NOTES

This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such

as IDs used by cashiers on point-of-sale terminals).

DEFINED APPROACH TESTING PROCEDURES

8.2.1.a Interview responsible personnel to verify that all users are assigned a unique ID for access to system components and cardholder data.

8.2.1.b Examine audit logs and other evidence to verify that access to system components and cardholder data can be uniquely identified and associated with individuals.

GUIDANCE

Purpose

The ability to trace actions performed on a computer system to an individual establishes accountability and traceability and is fundamental to establishing effective access controls.

By ensuring each user is uniquely identified, instead of using one ID for several employees, an organization can maintain individual responsibility for actions and an effective record in the audit log per employee. In addition, this will assist with issue resolution and containment when misuse or malicious intent occurs.

Good Practice

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:

- Account use is prevented unless needed for an exceptional circumstance.
- Use is limited to the time needed for the exceptional circumstance.
- Business justification for use is documented.
- Use is explicitly approved by management.
- Individual user identity is confirmed before access to an account is granted.
- Every action taken is attributable to an individual user.

CUSTOMIZED APPROACH OBJECTIVE

All actions performed by users with generic, system, or shared IDs are attributable to an individual person.

APPLICABILITY NOTES

This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

DEFINED APPROACH TESTING PROCEDURES

8.2.2.a Examine user account lists on system components and applicable documentation to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.

8.2.2.b Examine authentication policies and procedures to verify processes are defined for shared authentication credentials such that they are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.

8.2.2.c Interview system administrators to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Group, shared, or generic (or default) accounts are typically delivered with software or operating systems—for example, root or with privileges associated with a specific function, such as an administrator.

If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. In turn, this prevents an entity from assigning accountability for, or having effective logging of, an individual's actions since a given action could have been performed by anyone in the group with knowledge of the user ID and associated authentication factors.

The ability to associate individuals to the actions performed with an account is essential to provide individual accountability and traceability regarding who performed an action, what

action was performed, and when that action occurred.

Good Practice

If shared accounts are used for any reason, strong management controls need to be established to maintain individual accountability and traceability.

Definitions

Examples

Tools and techniques can facilitate both management and security of these types of accounts and confirm individual user identity before access to an account is granted. Entities can consider password vaults or other system-managed controls such as the sudo command.

An example of an exceptional circumstance is where all other authentication methods have failed, and a shared account is needed for emergency use or “break the glass” administrator access.

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.

CUSTOMIZED APPROACH OBJECTIVE

A service provider’s credential used for one customer cannot be used for any other customer.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement is not intended to apply to service providers accessing their own shared services environments, where multiple customer environments are hosted.

If service provider employees use shared authentication factors to remotely access customer premises, these factors must be unique per customer and managed in accordance with Requirement 8.2.2.

DEFINED APPROACH TESTING PROCEDURES

8.2.3 Additional testing procedure for service provider assessments only: Examine authentication policies and procedures and interview personnel to verify that service providers with remote access to customer premises use unique authentication factors for remote access to each customer premises.

GUIDANCE

Purpose

Service providers with remote access to customer premises typically use this access to support POS POI systems or provide other remote services.

If a service provider uses the same authentication factors to access multiple customers, all the service provider's customers can easily be compromised if an attacker compromises that one factor.

Criminals know this and deliberately target service providers looking for a shared authentication factor that gives them remote access to many merchants via that single factor.

Good Practice

Definitions

Examples

Technologies such as multi-factor mechanisms that provide a unique credential for each connection (such as a single-use password) could also meet the intent of this requirement.

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:

- Authorized with the appropriate approval.
- Implemented with only the privileges specified on the documented approval.

CUSTOMIZED APPROACH OBJECTIVE

Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.

APPLICABILITY NOTES

This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.

DEFINED APPROACH TESTING PROCEDURES

8.2.4 Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions) and examine system settings to verify the activity has been managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

It is imperative that the lifecycle of a user ID (additions, deletions, and modifications) is controlled so that only authorized accounts can perform functions, actions are auditable, and privileges are limited to only what is required.

Attackers often compromise an existing account and then escalate the privileges of that account to perform unauthorized acts, or they may create new IDs to continue their activity in the background. It is essential to detect and respond when user accounts are created or changed outside the normal change process or without corresponding authorization.

Good Practice

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.5 Access for terminated users is immediately revoked.

CUSTOMIZED APPROACH OBJECTIVE

The accounts of terminated users cannot be used.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.2.5.a Examine information sources for terminated users and review current user access lists—for both local and remote access—to verify that terminated user IDs have been deactivated or removed from the access lists.

8.2.5.b Interview responsible personnel to verify that all physical authentication factors—such as, smart cards, tokens, etc.—have been returned or deactivated for terminated users.

GUIDANCE

Purpose

If an employee or third party/vendor has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account.

Good Practice

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.

CUSTOMIZED APPROACH OBJECTIVE

Inactive user accounts cannot be used.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.2.6 Examine user accounts and last logon information, and interview personnel to verify that any inactive user accounts are removed or disabled within 90 days of inactivity.

GUIDANCE

Purpose

Accounts that are not used regularly are often targets of attack since it is less likely that any changes, such as a changed password, will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.

Good Practice

Where it may be reasonably anticipated that an account will not be used for an extended period of time, such as an extended leave of absence, the account should be disabled as soon as the leave begins, rather than waiting 90 days.

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:

- Enabled only during the time period needed and disabled when not in use.
- Use is monitored for unexpected activity.

CUSTOMIZED APPROACH OBJECTIVE

Third party remote access cannot be used except where specifically authorized and use is overseen by management.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.2.7 Interview personnel, examine documentation for managing accounts, and examine evidence to verify that accounts used by third parties for remote access are managed according to all elements specified in this requirement.

GUIDANCE

Purpose

Allowing third parties to have 24/7 access into an entity's systems and networks in case they need to provide support increases the chances of unauthorized access. This access could result in an unauthorized user in the third party's environment or a malicious individual using the always-available external entry point into an entity's network. Where third parties do need access 24/7, it should be documented, justified, monitored, and tied to specific service reasons.

Good Practice

Enabling access only for the time periods needed and disabling it as soon as it is no longer required helps prevent misuse of these connections. Additionally, consider assigning third parties a start and stop date for their access in accordance with their service contract. Monitoring third-party access helps ensure that third parties are accessing only the systems necessary and only during approved time frames. Any unusual activity using third-party accounts should be followed up and resolved.

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.

CUSTOMIZED APPROACH OBJECTIVE

A user session cannot be used except by the authorized user.

APPLICABILITY NOTES

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.

DEFINED APPROACH TESTING PROCEDURES

8.2.8 Examine system configuration settings to verify that system/session idle timeout features for user sessions have been set to 15 minutes or less.

GUIDANCE

Purpose

When users walk away from an open machine with access to system components or cardholder data, there is a risk that the machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse.

Good Practice

The re-authentication can be applied either at the system level to protect all sessions running on that machine or at the application level.

Entities may also want to consider staging controls in succession to further restrict the access of an unattended session as time passes. For example, the screensaver may activate after 15 minutes and log off the user after an hour.

However, timeout controls must balance the risk of access and exposure with the impact to the user and purpose of the access.

If a user needs to run a program from an unattended computer, the user can log in to the computer to initiate the program, and then "lock" the computer so that no one else can use the user's login while the computer is unattended.

Definitions

Examples

One way to meet this requirement is to configure an automated screensaver to launch whenever the console is idle for 15 minutes and requiring the logged-in user to enter their

password to unlock the screen.

Further Information

sections 8 | top

REQUIREMENTS and TESTING PROCEDURES 8.3

8.3 Strong authentication for users and administrators is established and managed.

DEFINED APPROACH REQUIREMENTS

8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a biometric element.

CUSTOMIZED APPROACH OBJECTIVE

An account cannot be accessed except with a combination of user identity and an authentication factor.

APPLICABILITY NOTES

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements.

A digital certificate is a valid option for “something you have” if it is unique for a particular user.

DEFINED APPROACH TESTING PROCEDURES

8.3.1.a Examine documentation describing the authentication factor(s) used to verify that user access to system components is authenticated via at least one authentication factor specified in this requirement.

8.3.1.b For each type of authentication factor used with each type of system component, observe an authentication to verify that authentication is functioning consistently with documented authentication factor(s).

GUIDANCE

Purpose

When used in addition to unique IDs, an authentication factor helps protect user IDs from being compromised, since the attacker needs to have the unique ID and compromise the associated authentication factor(s).

Good Practice

A common approach for a malicious individual to compromise a system is to exploit weak or nonexistent authentication factors (for example, passwords/passphrases). Requiring strong authentication factors helps protect against this attack.

Definitions

Examples

Further Information

See *fidoalliance.org* for more information about using tokens, smart cards, or biometrics as authentication factors.

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.

CUSTOMIZED APPROACH OBJECTIVE

Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.3.2.a Examine vendor documentation and system configuration settings to verify that authentication factors are rendered unreadable with strong cryptography during transmission and storage.

8.3.2.b Examine repositories of authentication factors to verify that they are unreadable during storage.

8.3.2.c Examine data transmissions to verify that authentication factors are unreadable during transmission.

GUIDANCE

Purpose

Network devices and applications have been known to transmit unencrypted, readable authentication factors (such as passwords and passphrases) across the network and/or store these values without encryption. As a result, a malicious individual can easily intercept this information during transmission using a “sniffer,” or directly access unencrypted authentication factors in files where they are stored, and then use this data to gain unauthorized access.

Good Practice

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.3 User identity is verified before modifying any authentication factor.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized individuals cannot gain system access by impersonating the identity of an authorized user.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.3.3 Examine procedures for modifying authentication factors and observe security personnel to verify that when a user requests a modification of an authentication factor, the user's identity is verified before the authentication factor is modified.

GUIDANCE

Purpose

Malicious individuals use "social engineering" techniques to impersonate a user of a system —for example, calling a help desk and acting as a legitimate user—to have an authentication factor changed so they can use a valid user ID.

Requiring positive identification of a user reduces the probability of this type of attack succeeding.

Good Practice

Modifications to authentication factors for which user identity should be verified include but are not limited to performing password resets, provisioning new hardware or software tokens, and generating new keys.

Definitions

Examples

Methods to verify a user's identity include a secret question/answer, knowledge-based information, and calling the user back at a known and previously established phone number.

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.4 Invalid authentication attempts are limited by:

- Locking out the user ID after not more than 10 attempts.
- Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

CUSTOMIZED APPROACH OBJECTIVE

An authentication factor cannot be guessed in a brute force, online attack.

APPLICABILITY NOTES

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

DEFINED APPROACH TESTING PROCEDURES

8.3.4.a Examine system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than 10 invalid logon attempts.

8.3.4.b Examine system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until the user's identity is confirmed.

GUIDANCE

Purpose

Without account-lockout mechanisms in place, an attacker can continually try to guess a password through manual or automated tools (for example, password cracking) until the attacker succeeds and gains access to a user's account.

If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of the locked account stop the malicious individual from guessing the password, as they will have to stop for a minimum of 30 minutes until the account is reactivated.

Good Practice

Before reactivating a locked account, the user's identity should be confirmed. For example, the administrator or help desk personnel can validate that the actual account owner is requesting reactivation, or there may be password reset self-service mechanisms that the account owner uses to verify their identity.

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:

- Set to a unique value for first-time use and upon reset.
- Forced to be changed immediately after the first use.

CUSTOMIZED APPROACH OBJECTIVE

An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.3.5 Examine procedures for setting and resetting passwords/passphrases (if used as authentication factors to meet Requirement 8.3.1) and observe security personnel to verify that passwords/passphrases are set and reset in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

If the same password/passphrase is used for every new user, an internal user, former employee, or malicious individual may know or easily discover the value and use it to gain access to accounts before the authorized user attempts to use the password.

Good Practice

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

CUSTOMIZED APPROACH OBJECTIVE

A guessed password/passphrase cannot be verified by either an online or offline brute force attack.

APPLICABILITY NOTES

This requirement is not intended to apply to: User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

- Application or system accounts, which are governed by requirements in section 8.6.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.

DEFINED APPROACH TESTING PROCEDURES

8.3.6 Examine system configuration settings to verify that user password/passphrase complexity parameters are set in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Strong passwords/passphrases may be the first line of defense into a network since a malicious individual will often first try to find accounts with weak, static, or non-existent passwords. If passwords are short or easily guessable, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID.

Good Practice

Password/passphrase strength is dependent on password/passphrase complexity, length, and randomness. Passwords/passphrases should be sufficiently complex, so they are

impractical for an attacker to guess or otherwise discover its value. Entities can consider adding increased complexity by requiring the use of special characters and upper- and lower-case characters, in addition to the minimum standards outlined by this requirement. Additional complexity increases the time required for offline brute force attacks of hashed passwords/passphrases.

Another option for increasing the resistance of passwords to guessing attacks is by comparing proposed password/passphrases to a bad password list and having users provide new passwords for any passwords found on the list.

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

CUSTOMIZED APPROACH OBJECTIVE

A previously used password cannot be used to gain access to an account for at least 12 months.

APPLICABILITY NOTES

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

DEFINED APPROACH TESTING PROCEDURES

8.3.7 Examine system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.

GUIDANCE

Purpose

If password history is not maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period reduces the likelihood that passwords that have been guessed or brute-forced will be re-used in the future.

Passwords or passphrases may have previously been changed due to suspicion of compromise or because the password or passphrase exceeded its effective use period, both of which are reasons why previously used passwords should not be reused.

Good Practice

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.8 Authentication policies and procedures are documented and communicated to all users including:

- Guidance on selecting strong authentication factors.
- Guidance for how users should protect their authentication factors.
- Instructions not to reuse previously used passwords/passphrases.
- Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

CUSTOMIZED APPROACH OBJECTIVE

Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.3.8.a Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.

8.3.8.b Review authentication policies and procedures that are distributed to users and verify they include the elements specified in this requirement.

8.3.8.c Interview users to verify that they are familiar with authentication policies and procedures.

GUIDANCE

Purpose

Communicating authentication policies and procedures to all users helps them to understand and abide by the policies.

Good Practice

Guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that do not contain dictionary words or information about the user, such as the user ID, names of family members, date of birth, etc.

Guidance for protecting authentication factors may include not writing down passwords or not saving them in insecure files, and being alert to malicious individuals who may try to exploit their passwords (for example, by calling an employee and asking for their password so the caller can “troubleshoot a problem”).

Alternatively, entities can implement processes to confirm passwords meet password policy, for example, by comparing password choices to a list of unacceptable passwords and having users choose a new password for any that match with one on the list. Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:

- Passwords/passphrases are changed at least once every 90 days,

OR

- The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

CUSTOMIZED APPROACH OBJECTIVE

An undetected compromised password/passphrase cannot be used indefinitely.

APPLICABILITY NOTES

This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements.

This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.

DEFINED APPROACH TESTING PROCEDURES

8.3.9 If passwords/passphrases are used as the only authentication factor for user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.

GUIDANCE

Purpose

Access to in-scope system components that are not in the CDE may be provided using a single authentication factor, such as a password/passphrase, token device or smart card, or biometric attribute. Where passwords/passphrases are employed as the only authentication factor for such access, additional controls are required to protect the integrity of the password/passphrase.

Good Practice

Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password.

Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase.

Dynamically analyzing an account's security posture is another option that allows for more rapid detection and response to address potentially compromised credentials. Such analysis takes a number of data points, which may include device integrity, location, access times, and the resources accessed to determine in real time whether an account can be granted access to a requested resource. In this way, access can be denied and accounts blocked if it is suspected that authentication credentials have been compromised.

Definitions

Examples

Further Information

For information about using dynamic analysis to manage user access to resources, see *NIST SP 800-207 Zero Trust Architecture*.

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.10 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including:

- Guidance for customers to change their user passwords/passphrases periodically.
- Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.

CUSTOMIZED APPROACH OBJECTIVE

Passwords/passphrases for service providers' customers cannot be used indefinitely.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement does not apply to accounts of consumer users accessing their own payment card information.

This requirement for service providers will be superseded by Requirement 8.3.10.1 once 8.3.10.1 becomes effective.

DEFINED APPROACH TESTING PROCEDURES

8.3.10 Additional testing procedure for service provider assessments only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data, examine guidance provided to customer users to verify that the guidance includes all elements specified in this requirement.

GUIDANCE

Purpose

Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase.

Good Practice

Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password.

Definitions

Examples

Further Information

sections 8 | top

REQUIREMENTS and TESTING PROCEDURES x.y

DEFINED APPROACH REQUIREMENTS

8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:

- Passwords/passphrases are changed at least once every 90 days,

OR

- The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

CUSTOMIZED APPROACH OBJECTIVE

Passwords/passphrases for service providers' customers cannot be used indefinitely.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement does not apply to accounts of consumer users accessing their own payment card information.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1.

DEFINED APPROACH TESTING PROCEDURES

8.3.10.1 Additional testing procedure for service provider assessments only: If passwords/passphrases are used as the only authentication factor for customer user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.

GUIDANCE

Purpose

Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase.

Good Practice

Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password.

Dynamically analyzing an account's security posture is another option that allows for more rapid detection and response to address potentially compromised credentials. Such analysis takes a number of data points which may include device integrity, location, access times, and the resources accessed to determine in real time whether an account can be granted access to a requested resource. In this way, access can be denied and accounts blocked if it is suspected that account credentials have been compromised.

Definitions

Examples

Further Information

For information about using dynamic analysis to manage user access to resources, refer to *NIST SP 800-207 Zero Trust Architecture*.

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used:

- Factors are assigned to an individual user and not shared among multiple users.
- Physical and/or logical controls ensure only the intended user can use that factor to gain access.

CUSTOMIZED APPROACH OBJECTIVE

An authentication factor cannot be used by anyone other than the user to which it is assigned.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

8.3.11.a Examine authentication policies and procedures to verify that procedures for using authentication factors such as physical security tokens, smart cards, and certificates are

defined and include all elements specified in this requirement.

8.3.11.b Interview security personnel to verify authentication factors are assigned to an individual user and not shared among multiple users.

8.3.11.c Examine system configuration settings and/or observe physical controls, as applicable, to verify that controls are implemented to ensure only the intended user can use that factor to gain access.

GUIDANCE

Purpose

If multiple users can use authentication factors such as tokens, smart cards, and certificates, it may be impossible to identify the individual using the authentication mechanism.

Good Practice

Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely authenticate the user of the account will prevent unauthorized users from gaining access to the user account through use of a shared authentication factor.

Definitions

Examples

Further Information

sections 8 | top

REQUIREMENTS and TESTING PROCEDURES 8.4

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

DEFINED APPROACH REQUIREMENTS

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.

CUSTOMIZED APPROACH OBJECTIVE

Administrative access to the CDE cannot be obtained by the use of a single authentication factor.

APPLICABILITY NOTES

The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection.

MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE.

DEFINED APPROACH TESTING PROCEDURES

8.4.1.a Examine network and/or system configurations to verify MFA is required for all non-console into the CDE for personnel with administrative access.

8.4.1.b Observe administrator personnel logging into the CDE and verify that MFA is required.

GUIDANCE

Purpose

Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase.

Good Practice

Definitions

Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.4.2 MFA is implemented for all access into the CDE.

CUSTOMIZED APPROACH OBJECTIVE

Access into the CDE cannot be obtained by the use of a single authentication factor.

APPLICABILITY NOTES

This requirement does not apply to:

- Application or system accounts performing automated functions.
- User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting via non-console administrative access from the entity's network into the CDE.

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function. MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

8.4.2.a Examine network and/or system configurations to verify MFA is implemented for all access into the CDE.

8.4.2.b Observe personnel logging in to the CDE and examine evidence to verify that MFA is required.

GUIDANCE

Purpose

Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase.

Good Practice

Definitions

Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:

- All remote access by all personnel, both users and administrators, originating from outside the entity's network.
- All remote access by third parties and vendors.

CUSTOMIZED APPROACH OBJECTIVE

Remote access to the entity's network cannot be obtained by using a single authentication factor.

APPLICABILITY NOTES

The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE.

If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to

networks with access to the CDE and is recommended for all remote access to the entity's networks.

The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.

DEFINED APPROACH TESTING PROCEDURES

8.4.3.a Examine network and/or system configurations for remote access servers and systems to verify MFA is required in accordance with all elements specified in this requirement.

8.4.3.b Observe personnel (for example, users and administrators) connecting remotely to the network and verify that multi-factor authentication is required.

GUIDANCE

Purpose

Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows, such as a password or passphrase.

Good Practice

Definitions

Multi-factor authentication (MFA) requires an individual to present a minimum of two of the three authentication factors specified in Requirement 8.3.1 before access is granted. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

Examples

Further Information

sections 8 | top

REQUIREMENTS and TESTING PROCEDURES 8.5

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

DEFINED APPROACH REQUIREMENTS

8.5.1 MFA systems are implemented as follows:

- The MFA system is not susceptible to replay attacks.
- MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.
- At least two different types of authentication factors are used.
- Success of all authentication factors is required before access is granted.

CUSTOMIZED APPROACH OBJECTIVE

MFA systems are resistant to attack and strictly control any administrative overrides.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

8.5.1.a Examine vendor system documentation to verify that the MFA system is not susceptible to replay attacks.

8.5.1.b Examine system configurations for the MFA implementation to verify it is configured in accordance with all elements specified in this requirement.

8.5.1.c Interview responsible personnel and observe processes to verify that any requests to bypass MFA are specifically documented and authorized by management on an exception basis, for a limited time period.

8.5.1.d Observe personnel logging into system components in the CDE to verify that access is granted only after all authentication factors are successful.

8.5.1.e Observe personnel connecting remotely from outside the entity’s network to verify that access is granted only after all authentication factors are successful.

GUIDANCE

Purpose

Poorly configured MFA systems can be bypassed by attackers. This requirement therefore addresses configuration of MFA system(s) that provide MFA for users accessing system components in the CDE.

Good Practice

Definitions

Using one type of factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

Examples

Further Information

For more information about MFA systems and features, refer to the following:

PCI SSC's *Information Supplement: Multi-Factor Authentication*

PCI SSC's Frequently Asked Questions (FAQs) on this topic.

sections 8 | top

REQUIREMENTS and TESTING PROCEDURES 8.6

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

DEFINED APPROACH REQUIREMENTS

8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows:

- Interactive use is prevented unless needed for an exceptional circumstance.
- Interactive use is limited to the time needed for the exceptional circumstance.
- Business justification for interactive use is documented.
- Interactive use is explicitly approved by management.
- Individual user identity is confirmed before access to account is granted.
- Every action taken is attributable to an individual user.

CUSTOMIZED APPROACH OBJECTIVE

When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

8.6.1 Examine application and system accounts that can be used interactively and interview administrative personnel to verify that application and system accounts are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Like individual user accounts, system and application accounts require accountability and strict management to ensure they are used only for the intended purpose and are not misused. Attackers often compromise system or application accounts to gain access to cardholder data.

Good Practice

Where possible, configure system and application accounts to disallow interactive login to prevent unauthorized individuals from logging in and using the account with its associated system privileges, and to limit the machines and devices on which the account can be used.

Definitions

System or application accounts are those accounts that execute processes or perform tasks on a computer system or application and are not typically accounts that an individual logs into. These accounts usually have elevated privileges that are required to perform specialized tasks or functions.

Interactive login is the ability for a person to log into a system or application account in the same manner as a normal user account. Using system and application accounts this way means there is no accountability and traceability of actions taken by the user.

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.

CUSTOMIZED APPROACH OBJECTIVE

Passwords/passphrases used by application and system accounts cannot be used by unauthorized personnel.

APPLICABILITY NOTES

Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

8.6.2.a Interview personnel and examine system development procedures to verify that processes are defined for application and system accounts that can be used for interactive login, specifying that passwords/passphrases are not hard coded in scripts, configuration/property files, or bespoke and custom source code.

8.6.2.b Examine scripts, configuration/property files, and bespoke and custom source code for application and system accounts that can be used for interactive login, to verify passwords/passphrases for those accounts are not present.

GUIDANCE

Purpose

Not properly protecting passwords/passphrases used by application and system accounts, especially if those accounts can be used for interactive login, increases the risk and success of unauthorized use of those privileged accounts.

Good Practice

Changing these values due to suspected or confirmed disclosure can be particularly difficult to implement. Tools can facilitate both management and security of authentication factors

for application and system accounts. For example, consider password vaults or other system-managed controls.

Definitions

Examples

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:

- Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.
- Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.

CUSTOMIZED APPROACH OBJECTIVE

Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

8.6.3.a Examine policies and procedures to verify that procedures are defined to protect passwords/passphrases for application or system accounts against misuse in accordance with all elements specified in this requirement.

8.6.3.b Examine the entity's targeted risk analysis for the change frequency and complexity for passwords/passphrases used for interactive login to application and system accounts to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1 and addresses:

- The frequency defined for periodic changes to application and system passwords/passphrases.
- The complexity defined for passwords/passphrases and appropriateness of the complexity relative to the frequency of changes.

8.6.3.c Interview responsible personnel and examine system configuration settings to verify that passwords/passphrases for any application and system accounts that can be used for interactive login are protected against misuse in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Systems and application accounts pose more inherent security risk than user accounts because they often run in an elevated security context, with access to systems that may not be typically granted to user accounts, such as programmatic access to databases, etc. As a result, special consideration must be made to protect passwords/passphrases used for application and system accounts.

Good Practice

Entities should consider the following risk factors when determining how to protect application and system passwords/passphrases against misuse:

- How securely the passwords/passphrases are stored (for example, whether they are stored in a password vault).
- Staff turnover.
- The number of people with access to the authentication factor.
- Whether the account can be used for interactive login.
- Whether the security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly (see Requirement 8.3.9).

All these elements affect the level of risk for application and system accounts and might impact the security of systems accessed by the system and application accounts.

Entities should correlate their selected change frequency for application and system passwords/passwords with their selected complexity for those passwords/passphrases – i.e., the complexity should be more rigorous when passwords/passphrases are changed infrequently and can be less rigorous when changed more frequently. For example, a longer change frequency is more justifiable when passwords/passphrases complexity is set

to 36 alphanumeric characters with upper- and lower-case letters, numbers, and special characters.

Best practices are to consider password changes at least once a year, a password/passphrase length of at least 15 characters, and complexity for the passwords/passphrase of alphanumeric characters, with upper- and lower-case letters, and special characters.

Definitions

Examples

Further Information

For information about variability and equivalency of password strength for passwords/passphrases of different formats, see the industry standards (for example, the current version of *NIST SP 800-63 Digital Identity Guidelines*).

sections 8 | top

PRINCIPLE PCI DSS REQUIREMENT: Implement Strong Access Control Measures

Requirement 9: Restrict Physical Access to Cardholder Data

OVERVIEW

Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

There are three different areas mentioned in Requirement 9:

1. Requirements that specifically refer to sensitive areas are intended to apply to those areas only.

2. Requirements that specifically refer to the cardholder data environment (CDE) are intended to apply to the entire CDE, including any sensitive areas residing within the CDE.
3. Requirements that specifically refer to the facility are referencing the types of controls that may be managed more broadly at the physical boundary of a business premise (such as a building) within which CDEs and sensitive areas reside. These controls often exist outside a CDE or sensitive area, for example a guard desk that identifies, badges, and logs visitors. The term “facility” is used to recognize that these controls may exist at different places within a facility, for instance, at building entry or at an internal entrance to a data center or office space.

Refer to Appendix G for definitions of “media,” “personnel,” “sensitive areas” and other PCI DSS terms.

SECTIONS 9

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

requirement 9 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 9.1

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

DEFINED APPROACH REQUIREMENTS

9.1.1 All security policies and operational procedures that are identified in Requirement 9 are:

- Documented.

- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 9 are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 9.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 9. While it is important to define the specific policies or procedures called out in Requirement 9, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 9 are documented and assigned.

9.1.2.b Interview personnel with responsibility for performing activities in Requirement 9 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Definitions

Examples

Further Information

sections 9 | top

REQUIREMENTS and TESTING PROCEDURES 9.2

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

DEFINED APPROACH REQUIREMENTS

9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.

CUSTOMIZED APPROACH OBJECTIVE

9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.2.1 Observe entry controls and interview responsible personnel to verify that physical security controls are in place to restrict access to systems in the CDE.

GUIDANCE

Purpose

Without physical access controls, unauthorized persons could potentially gain access to the CDE and sensitive information, or could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment. Therefore, the purpose of this requirement is that physical access to the CDE is controlled via physical security controls such as badge readers or other mechanisms such as lock and key.

Good Practice

Whichever mechanism meets this requirement, it must be sufficient for the organization to verify that only authorized personnel are granted

Definitions

Examples

Facility entry controls include physical security controls at each computer room, data center, and other physical areas with systems in the CDE. It can also include badge readers or other devices that manage physical access controls, such as lock and key with a current list of all individuals holding the keys.

Further Information

sections 8 | top

DEFINED APPROACH REQUIREMENTS

9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:

- Entry and exit points to/from sensitive areas within the CDE are monitored.
- Monitoring devices or mechanisms are protected from tampering or disabling.
- Collected data is reviewed and correlated with other entries.
- Collected data is stored for at least three months, unless otherwise restricted by law.

CUSTOMIZED APPROACH OBJECTIVE

Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.2.1.1.a Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are in place to monitor the entry and exit points.

9.2.1.1.b Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are protected from tampering or disabling.

9.2.1.1.c Observe the physical access control mechanisms and/or examine video cameras and interview responsible personnel to verify that:

- Collected data from video cameras and/or physical access control mechanisms is reviewed and correlated with other entries.
- Collected data is stored for at least three months.

GUIDANCE

Purpose

Maintaining details of individuals entering and exiting the sensitive areas can help with investigations of physical breaches by identifying individuals that physically accessed the sensitive areas, as well as when they entered and exited.

Good Practice

Whichever mechanism meets this requirement, it should effectively monitor all entry and exit points to sensitive areas.

Criminals attempting to gain physical access to sensitive areas will often try to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, physical access control mechanisms could be monitored or have physical protections installed to prevent them from being damaged or disabled by malicious individuals.

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized devices cannot connect to the entity's network from public areas within the facility.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.2.2 Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks within the facility.

GUIDANCE

Purpose

Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gaining access to the CDE or systems connected to the CDE.

Good Practice

Whether logical or physical controls, or a combination of both, are used, they should prevent an individual or device that is not explicitly authorized from being able to connect to the network.

Definitions

Examples

Methods to meet this requirement include network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.

CUSTOMIZED APPROACH OBJECTIVE

Physical networking equipment cannot be accessed by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.2.3 Interview responsible personnel and observe locations of hardware and lines to verify that physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.

GUIDANCE

Purpose

Without appropriate physical security over access to wireless components and devices, and computer networking and telecommunications equipment and lines, malicious users could gain access to the entity's network resources. Additionally, they could connect their own devices to the network to gain unauthorized access to the CDE or systems connected to the CDE.

Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.

CUSTOMIZED APPROACH OBJECTIVE

Physical consoles within sensitive areas cannot be used by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.2.4 Observe a system administrator's attempt to log into consoles in sensitive areas and verify that they are "locked" to prevent unauthorized use.

GUIDANCE

Purpose

Locking console login screens prevents unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

REQUIREMENTS and TESTING PROCEDURES 9.3

9.3 Physical access for personnel and visitors is authorized and managed.

DEFINED APPROACH REQUIREMENTS

9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:

- Identifying personnel.
- Managing changes to an individual's physical access requirements.
- Revoking or terminating personnel identification.
- Limiting access to the identification process or system to authorized personnel.

CUSTOMIZED APPROACH OBJECTIVE

Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.3.1.a Examine documented procedures to verify that procedures to authorize and manage physical access of personnel to the CDE are defined in accordance with all elements specified in this requirement.

9.3.1.b Observe identification methods, such as ID badges, and processes to verify that personnel in the CDE are clearly identified.

9.3.1.c Observe processes to verify that access to the identification process, such as a badge system, is limited to authorized personnel.

GUIDANCE

Purpose

Establishing procedures for granting, managing, and removing access when it is no longer needed ensures non-authorized individuals are prevented from gaining access to areas containing cardholder data. In addition, it is important to limit access to the actual badging system and badging materials to prevent unauthorized personnel from making their own badges and/or setting up their own access rules.

Good Practice

It is important to visually identify the personnel that are physically present, and whether the individual is a visitor or an employee.

Definitions

Examples

One way to identify personnel is to assign them badges.

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows:

- Access is authorized and based on individual job function.
- Access is revoked immediately upon termination.

- All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.

CUSTOMIZED APPROACH OBJECTIVE

Sensitive areas cannot be accessed by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.3.1.1.a Observe personnel in sensitive areas within the CDE, interview responsible personnel, and examine physical access control lists to verify that:

- Access to the sensitive area is authorized.
- Access is required for the individual's job function. 9.3.1.1.b Observe processes and interview personnel to verify that access of all personnel is revoked immediately upon termination.

9.3.1.1.c For terminated personnel, examine physical access controls lists and interview responsible personnel to verify that all physical access mechanisms (such as keys, access cards, etc.) were returned or disabled.

GUIDANCE

Purpose

Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access.

Good Practice

Where possible, organizations should have policies and procedures to ensure that before personnel leaving the organization, all physical access mechanisms are returned, or disabled as soon as possible upon their departure. This will ensure personnel cannot gain physical access to sensitive areas once their employment has ended.

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including:

- Visitors are authorized before entering.
- Visitors are escorted at all times.
- Visitors are clearly identified and given a badge or other identification that expires.
- Visitor badges or other identification visibly distinguishes visitors from personnel.

CUSTOMIZED APPROACH OBJECTIVE

Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.3.2.a Examine documented procedures and interview personnel to verify procedures are defined for authorizing and managing visitor access to the CDE in accordance with all elements specified in this requirement. 9.3.2.b Observe processes when visitors are present in the CDE and interview personnel to verify that visitors are:

- Authorized before entering the CDE.
- Escorted at all times within the CDE. 9.3.2.c Observe the use of visitor badges or other identification to verify that the badge or other identification does not permit unescorted access to the CDE. 9.3.2.d Observe visitors in the CDE to verify that:
- Visitor badges or other identification are being used for all visitors.
- Visitor badges or identification easily distinguish visitors from personnel. 9.3.2.e Examine visitor badges or other identification and observe evidence in the badging system to verify visitor badges or other identification expires.

GUIDANCE

Purpose

Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities and potentially to cardholder data.

Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.

CUSTOMIZED APPROACH OBJECTIVE

Visitor identification or badges cannot be reused after expiration.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.3.3 Observe visitors leaving the facility and interview personnel to verify visitor badges or other identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. upon departure or expiration.

GUIDANCE

Purpose

Ensuring that visitor badges are returned or deactivated upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including:

- The visitor's name and the organization represented.
- The date and time of the visit.
- The name of the personnel authorizing physical access.
- Retaining the log for at least three months, unless otherwise restricted by law.

CUSTOMIZED APPROACH OBJECTIVE

Records of visitor access that enable the identification of individuals are maintained.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.3.4.a Examine the visitor log and interview responsible personnel to verify that a visitor log is used to record physical access to the facility and sensitive areas.

9.3.4.b Examine the visitor log and verify that the log contains:

- The visitor's name and the organization represented.
- The personnel authorizing physical access.
- Date and time of visit.

9.3.4.c Examine visitor log storage locations and interview responsible personnel to verify that the log is retained for at least three months, unless otherwise restricted by law.

GUIDANCE

Purpose

A visitor log documenting minimum information about the visitor is easy and inexpensive to maintain. It will assist in identifying historical physical access to a building or room and potential access to cardholder data.

Good Practice

When logging the date and time of visit, including both in and out times is considered a best practice, since it provides helpful tracking information and provides assurance that a visitor has left at the end of the day. It is also good to verify that a visitor's ID (driver's license, etc.) matches the name they put on the visitor log.

Definitions

Examples

Further Information

sections 9 | top

REQUIREMENTS and TESTING PROCEDURES 9.4

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

DEFINED APPROACH REQUIREMENTS

9.4.1 All media with cardholder data is physically secured.

CUSTOMIZED APPROACH OBJECTIVE

Media with cardholder data cannot be accessed by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.1. Examine documentation to verify that the procedures defined for protecting cardholder data include controls for physically securing all media.

GUIDANCE

Purpose

Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone’s desk.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.1.1 Offline media backups with cardholder data are stored in a secure location.

CUSTOMIZED APPROACH OBJECTIVE

Offline backups cannot be accessed by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.1.1.a Examine documentation to verify that procedures are defined for physically securing offline media backups with cardholder data in a secure location.

9.4.1.1.b Examine logs or other documentation and interview responsible personnel at the storage location to verify that offline media backups are stored in a secure location.

GUIDANCE

Purpose

If stored in a non-secured facility, backups containing cardholder data may easily be lost, stolen, or copied for malicious intent.

Good Practice

For secure storage of backup media, a good practice is to store media in an off-site facility, such as an alternate or backup site or commercial storage facility.

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.

CUSTOMIZED APPROACH OBJECTIVE

The security controls protecting offline backups are verified periodically by inspection.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.1.2.a Examine documentation to verify that procedures are defined for reviewing the security of the offline media backup location(s) with cardholder data at least once every 12 months.

9.4.1.2.b Examine documented procedures, logs, or other documentation, and interview responsible personnel at the storage location(s) to verify that the storage location's security is reviewed at least once every 12 months.

GUIDANCE

Purpose

Conducting regular reviews of the storage facility enables the organization to address identified security issues promptly, minimizing the potential risk. It is important for the entity to be aware of the security of the area where media is being stored.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.

CUSTOMIZED APPROACH OBJECTIVE

Media are classified and protected appropriately.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.2.a Examine documentation to verify that procedures are defined for classifying media with cardholder data in accordance with the sensitivity of the data.

9.4.2.b Examine media logs or other documentation to verify that all media is classified in accordance with the sensitivity of the data.

GUIDANCE

Purpose

Media not identified as confidential may not be adequately protected or may be lost or stolen.

Good Practice

It is important that media be identified such that its classification status is apparent. This does not mean however that the media needs to have a “confidential” label.

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.3 Media with cardholder data sent outside the facility is secured as follows:

- Media sent outside the facility is logged.
- Media is sent by secured courier or other delivery method that can be accurately tracked.
- Offsite tracking logs include details about media location.

CUSTOMIZED APPROACH OBJECTIVE

Media is secured and tracked when transported outside the facility.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.3.a Examine documentation to verify that procedures are defined for securing media sent outside the facility in accordance with all elements specified in this requirement.

9.4.3.b Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.

9.4.3.c Examine offsite tracking logs for all media to verify tracking details are documented.

GUIDANCE

Purpose

Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. The use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).

CUSTOMIZED APPROACH OBJECTIVE

Media cannot leave a facility without the approval of accountable personnel.

APPLICABILITY NOTES

Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have “manager” as part of their title.

DEFINED APPROACH TESTING PROCEDURES

9.4.4.a Examine documentation to verify that procedures are defined to ensure that media moved outside the facility is approved by management.

9.4.4.b Examine offsite media tracking logs and interview responsible personnel to verify that proper management authorization is obtained for all media moved outside the facility (including media distributed to individuals).

GUIDANCE

Purpose

Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.5 Inventory logs of all electronic media with cardholder data are maintained.

CUSTOMIZED APPROACH OBJECTIVE

Accurate inventories of stored electronic media are maintained.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.5.a Examine documentation to verify that procedures are defined to maintain electronic media inventory logs.

9.4.5.b Examine electronic media inventory logs and interview responsible personnel to verify that logs are maintained.

GUIDANCE

Purpose

Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.

CUSTOMIZED APPROACH OBJECTIVE

Media inventories are verified periodically.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.4.5.1.a Examine documentation to verify that procedures are defined to conduct inventories of electronic media with cardholder data at least once every 12 months.

9.4.5.1.b Examine electronic media inventory logs and interview personnel to verify that electronic media inventories are performed at least once every 12 months.

GUIDANCE

Purpose

Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.

Good Practice

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:

- Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
- Materials are stored in secure storage containers prior to destruction.

CUSTOMIZED APPROACH OBJECTIVE

Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.

APPLICABILITY NOTES

These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.

DEFINED APPROACH TESTING PROCEDURES

9.4.6.a Examine the periodic media destruction policy to verify that procedures are defined to destroy hard-copy media with cardholder data when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.

9.4.6.b Observe processes and interview personnel to verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that cardholder data cannot be reconstructed.

9.4.6.c Observe storage containers used for materials that contain information to be destroyed to verify that the containers are secure.

GUIDANCE

Purpose

If steps are not taken to destroy information contained on hard-copy media before disposal, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins looking for hard-copy materials with information they can use to launch an attack.

Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being capture

Good Practice

Consider “to-be-shredded” containers with a lock that prevents access to its contents or that physically prevent access to the inside of the container.

Definitions

Examples

Further Information

See *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*.

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:

- The electronic media is destroyed.
- The cardholder data is rendered unrecoverable so that it cannot be reconstructed.

CUSTOMIZED APPROACH OBJECTIVE

Cardholder data cannot be recovered from media that has been erased or destroyed.

APPLICABILITY NOTES

These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1,

which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.

DEFINED APPROACH TESTING PROCEDURES

9.4.7.a Examine the periodic media destruction policy to verify that procedures are defined to destroy electronic media when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.

9.4.7.b Observe the media destruction process and interview responsible personnel to verify that electronic media with cardholder data is destroyed via one of the methods specified in this requirement.

GUIDANCE

Purpose

If steps are not taken to destroy information contained on electronic media when no longer needed, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack.

Good Practice

The deletion function in most operating systems allows deleted data to be recovered, so instead, a dedicated secure deletion function or application should be used to make data unrecoverable.

Definitions

Examples

Methods for securely destroying electronic media include secure wiping in accordance with industry-accepted standards for secure deletion, degaussing, or physical destruction (such as grinding or shredding hard disks).

Further Information

See *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*.

sections 9 | top

REQUIREMENTS and TESTING PROCEDURES 9.5

9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

DEFINED APPROACH REQUIREMENTS

9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

- Maintaining a list of POI devices.
- Periodically inspecting POI devices to look for tampering or unauthorized substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

CUSTOMIZED APPROACH OBJECTIVE

The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.

APPLICABILITY NOTES

These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). This requirement is not intended to apply to manual PAN key-entry components such as computer keyboards.

This requirement is recommended, but not required, for manual PAN key-entry components such as computer keyboards.

This requirement does not apply to commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.

DEFINED APPROACH TESTING PROCEDURES

9.5.1 Examine documented policies and procedures to verify that processes are defined that include all elements specified in this requirement.

GUIDANCE

Purpose

Criminals attempt to steal payment card data by stealing and/or manipulating card-reading devices and terminals. Criminals will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card data every time a card is entered.

They will also try to add “skimming” components to the outside of devices, which are designed to capture payment card data before it enters the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card data is captured twice: once by the criminal’s component and then by the device’s legitimate component. In this way, transactions may still be completed without interruption while the criminal is “skimming” the payment card data during the process.

Good Practice

Definitions

Examples

Further Information

Additional best practices on skimming prevention are available on the PCI SSC website.

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.5.1.1 An up-to-date list of POI devices is maintained, including:

- Make and model of the device.
- Location of device.
- Device serial number or other methods of unique identification.

CUSTOMIZED APPROACH OBJECTIVE

The identity and location of POI devices is recorded and known at all times.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.5.1.1.a Examine the list of POI devices to verify it includes all elements specified in this requirement.

9.5.1.1.b Observe POI devices and device locations and compare to devices in the list to verify that the list is accurate and up to date.

9.5.1.1.c Interview personnel to verify the list of POI devices is updated when devices are added, relocated, decommissioned, etc.

GUIDANCE

Purpose

Keeping an up-to-date list of POI devices helps an organization track where devices are supposed to be and quickly identify if a device is missing or lost.

Good Practice

The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned.

Definitions

Examples

Methods to maintain device locations include identifying the address of the site or facility where the device is located.

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

CUSTOMIZED APPROACH OBJECTIVE

Point of Interaction Devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.5.1.2.a Examine documented procedures to verify processes are defined for periodic inspections of POI device surfaces to detect tampering and unauthorized substitution.

9.5.1.2.b Interview responsible personnel and observe inspection processes to verify:

- Personnel are aware of procedures for inspecting devices.
- All devices are periodically inspected for evidence of tampering and unauthorized substitution.

GUIDANCE

Purpose

Regular inspections of devices will help organizations detect tampering more quickly via external evidence—for example, the addition of a card skimmer—or replacement of a device, thereby minimizing the potential impact of using fraudulent devices.

Good Practice

Methods for periodic inspection include checking the serial number or other device characteristics and comparing the information to the list of POI devices to verify the device has not been swapped with a fraudulent device.

Definitions

Examples

The type of inspection will depend on the device. For instance, photographs of devices known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also provide security guidance and "how to" guides to help determine whether the device has been subject to tampering.

Signs that a device might have been tampered with or substituted include:

- Unexpected attachments or cables plugged into the device.
- Missing or changed security labels.

- Broken or differently colored casing.
- Changes to the serial number or other external markings.

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

CUSTOMIZED APPROACH OBJECTIVE

POI devices are inspected at a frequency that addresses the entity's risk.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

9.5.1.2.1.a Examine the entity's targeted risk analysis for the frequency of periodic POI device inspections and type of inspections performed to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.

9.5.1.2.1.b Examine documented results of periodic device inspections and interview personnel to verify that the frequency and type of POI device inspections performed match what is defined in the entity's targeted risk analysis conducted for this requirement.

GUIDANCE

Purpose

Entities are best placed to determine the frequency of POI device inspections based on the environment in which the device operates.

Good Practice

The frequency of inspections will depend on factors such as the location of a device and whether the device is attended or unattended. For example, devices left in public areas

without supervision by the organization's personnel might have more frequent inspections than devices kept in secure areas or supervised when accessible to the public. In addition, many POI vendors include guidance in their user documentation about how often POI devices should be checked, and for what – entities should consult their vendors' documentation and incorporate those recommendations into their periodic inspections.

Definitions

Examples

Further Information

sections 9 | top

DEFINED APPROACH REQUIREMENTS

9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

CUSTOMIZED APPROACH OBJECTIVE

Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

9.5.1.3.a Review training materials for personnel in POI environments to verify they include all elements specified in this requirement.

9.5.1.3.b Interview personnel in POI environments to verify they have received training and know the procedures for all elements specified in this requirement.

GUIDANCE

Purpose

Criminals will often pose as authorized maintenance personnel to gain access to POI devices.

Good Practice

Personnel training should include being alert to and questioning anyone who shows up to do POI maintenance to ensure they are authorized and have a valid work order, including any agents, maintenance or repair personnel, technicians, service providers, or other third parties. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POI maintenance company, such as the vendor or acquirer, for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work apparel), and could also be knowledgeable about locations of devices, so personnel should be trained to always follow procedures.

Another trick that criminals use is to send a “new” POI device with instructions for swapping it with a legitimate device and “returning” the legitimate device. The criminals may even provide return postage to their specified address. Therefore, personnel should always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business.

Definitions

Examples

Suspicious behavior that personnel should be aware of includes attempts by unknown persons to unplug or open devices.

Ensuring personnel are aware of mechanisms for reporting suspicious behavior and who to report such behavior to—for example, a manager or security officer—will help reduce the likelihood and potential impact of a device being tampered with or substituted.

Further Information

sections 9 | top

PRINCIPLE PCI DSS REQUIREMENT: Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

OVERVIEW

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.

This requirement applies to user activities, including those by employees, contractors, consultants, and internal and external vendors, and other third parties (for example, those providing support or maintenance services).

These requirements do not apply to user activity of consumers (cardholders).

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 10

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

REQUIREMENTS and TESTING PROCEDURES 10.1

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

DEFINED APPROACH REQUIREMENTS

10.1.1 All security policies and operational procedures that are identified in Requirement 10 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

APPLICABILITY NOTES

10.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 10 are managed in accordance with all elements specified in this requirement.

DEFINED APPROACH TESTING PROCEDURES

Requirement 10.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 10. While it is important to define the specific policies or procedures called out in Requirement 10, it is equally important to ensure they are properly documented, maintained, and disseminated.

GUIDANCE

Purpose

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Good Practice

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 10 are documented and assigned.

10.1.2.b Interview personnel with responsibility for performing activities in Requirement 10 to verify that roles and responsibilities are assigned as defined and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 10 | top

REQUIREMENTS and TESTING PROCEDURES 10.2

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

DEFINED APPROACH REQUIREMENTS

10.2.1 Audit logs are enabled and active for all system components and cardholder data.

CUSTOMIZED APPROACH OBJECTIVE

Records of all activities affecting system components and cardholder data are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1 Interview the system administrator and examine system configurations to verify that audit logs are enabled and active for all system components.

GUIDANCE

Purpose

Audit logs must exist for all system components. Audit logs send alerts the system administrator, provides data to other monitoring mechanisms, such as intrusion-detection systems (IDS) and security information and event monitoring systems (SIEM) tools, and provide a history trail for post-incident investigation.

Logging and analyzing security-relevant events enable an organization to identify and trace potentially malicious activities.

Good Practice

When an entity considers which information to record in their logs, it is important to remember that information stored in audit logs is sensitive and should be protected per requirements in this standard. Care should be taken to only store essential information in the audit logs to minimize risk.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.1.1 Audit logs capture all individual user access to cardholder data.

CUSTOMIZED APPROACH OBJECTIVE

Records of all individual user access to cardholder data are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.1 Examine audit log configurations and log data to verify that all individual user access to cardholder data is logged.

GUIDANCE

Purpose

It is critical to have a process or system that links user access to system components accessed. Malicious individuals could obtain knowledge of a user account with access to

systems in the CDE, or they could create a new, unauthorized account to access cardholder data.

Good Practice

A record of all individual access to cardholder data can identify which accounts may have been compromised or misused.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

A record of all individual access to cardholder data can identify which accounts may have been compromised or misused.

CUSTOMIZED APPROACH OBJECTIVE

Records of all actions performed by individuals with elevated privileges are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.2 Examine audit log configurations and log data to verify that all actions taken by any individual with administrative access, including any interactive use of application or system accounts, are logged.

GUIDANCE

Purpose

Accounts with increased access privileges, such as the “administrator” or “root” account, have the potential to significantly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is cannot trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and account.

Good Practice

Definitions

Accounts with administrative access are those assigned with specific privileges or abilities for that account to manage systems, networks, and/or applications. The functions or activities considered to be administrative are beyond those performed by regular users as part of routine business functions.

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.1.3 Audit logs capture all access to audit logs.

CUSTOMIZED APPROACH OBJECTIVE

Records of all access to audit logs are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.3 Examine audit log configurations and log data to verify that access to all audit logs is captured.

GUIDANCE

Purpose

Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having logs identify changes, additions, and deletions to the audit logs can help retrace steps made by unauthorized personnel.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.1.4 Audit logs capture all invalid logical access attempts.

CUSTOMIZED APPROACH OBJECTIVE

Records of all invalid access attempts are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.4 Examine audit log configurations and log data to verify that invalid logical access attempts are captured.

GUIDANCE

Purpose

Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user’s attempts to “brute force” or guess a password.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to:

- Creation of new accounts.
- Elevation of privileges.
- All changes, additions, or deletions to accounts with administrative access.

CUSTOMIZED APPROACH OBJECTIVE

Records of all changes to identification and authentication credentials are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.5 Examine audit log configurations and log data to verify that changes to identification and authentication credentials are captured in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Logging changes to authentication credentials (including elevation of privileges, additions, and deletions of accounts with administrative access) provides residual evidence of activities.

Malicious users may attempt to manipulate authentication credentials to bypass them or impersonate a valid account.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.1.6 Audit logs capture the following:

- All initialization of new audit logs, and
- All starting, stopping, or pausing of the existing audit logs.

CUSTOMIZED APPROACH OBJECTIVE

Records of all changes to audit log activity status are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.6 Examine audit log configurations and log data to verify that all elements specified in this requirement are captured.

GUIDANCE

Purpose

Turning off or pausing audit logs before performing illicit activities is common practice for malicious users who want to avoid detection. Initialization of audit logs could indicate that that a user disabled the log function to hide their actions.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.1.7 Audit logs capture all creation and deletion of system-level objects.

CUSTOMIZED APPROACH OBJECTIVE

Records of alterations that indicate a system has been modified from its intended functionality are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.1.7 Examine audit log configurations and log data to verify that creation and deletion of system level objects is captured.

GUIDANCE

Purpose

Malicious software, such as malware, often creates or replaces system-level objects on the target system to control a particular function or operation on that system. By logging when system-level objects are created or deleted, it will be easier to determine whether such modifications were authorized.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.2.2 Audit logs record the following details for each auditable event:

- User identification.
- Type of event.
- Date and time.
- Success and failure indication.
- Origination of event.
- Identity or name of affected data, system component, resource, or service (for example, name and protocol).

CUSTOMIZED APPROACH OBJECTIVE

Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.2.2 Interview personnel and examine audit log configurations and log data to verify that all elements specified in this requirement are included in log entries for each auditable event (from 10.2.1.1 through 10.2.1.7).

GUIDANCE

Purpose

By recording these details for the auditable events at 10.2.1.1 through 10.2.1.7, a potential compromise can be quickly identified, with sufficient detail to facilitate following up on suspicious activities.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

REQUIREMENTS and TESTING PROCEDURES 10.3

10.3 Audit logs are protected from destruction and unauthorized modifications.

DEFINED APPROACH REQUIREMENTS

10.3.1 Read access to audit logs files is limited to those with a job-related need.

CUSTOMIZED APPROACH OBJECTIVE

Stored activity records cannot be accessed by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.3.1 Interview system administrators and examine system configurations and privileges to verify that only individuals with a job-related need have read access to audit log files.

GUIDANCE

Purpose

Audit log files contain sensitive information, and read access to the log files must be limited only to those with a valid business need. This access includes audit log files on the originating systems as well as anywhere else they are stored.

Good Practice

Adequate protection of the audit logs includes strong access control that limits access to logs based on “need to know” only and the use of physical or network segregation to make the logs harder to find and modify.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.3.2 Audit log files are protected to prevent modifications by individuals.

CUSTOMIZED APPROACH OBJECTIVE

Stored activity records cannot be modified by personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.3.2 Examine system configurations and privileges and interview system administrators to verify that current audit log files are protected from modifications by individuals via access control mechanisms, physical segregation, and/or network segregation.

GUIDANCE

Purpose

Often a malicious individual who has entered the network will try to edit the audit logs to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise. Therefore, audit logs should be protected on the originating systems as well as anywhere else they are stored.

Good Practice

Entities should attempt to prevent logs from being exposed in public-accessible locations.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.

CUSTOMIZED APPROACH OBJECTIVE

Stored activity records are secured and preserved in a central location to prevent unauthorized modification.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.3.3 Examine backup configurations or log files to verify that current audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.

GUIDANCE

Purpose

Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected, even if the system generating the logs becomes compromised.

Writing logs from external-facing technologies such as wireless, network security controls, DNS, and mail servers, reduces the risk of those logs being lost or altered.

Good Practice

Each entity determines the best way to back up log files, whether via one or more centralized log servers or other secure media. Logs may be written directly, offloaded, or copied from external systems to the secure internal system or media.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.

CUSTOMIZED APPROACH OBJECTIVE

Stored activity records cannot be modified without an alert being generated.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.3.4 Examine system settings, monitored files, and results from monitoring activities to verify the use of file integrity monitoring or change-detection software on audit logs.

GUIDANCE

Purpose

File integrity monitoring or change-detection systems check for changes to critical files and notify when such changes are identified. For file integrity monitoring purposes, an entity usually monitors files that do not regularly change, but when changed, indicate a possible compromise.

Good Practice

Software used to monitor changes to audit logs should be configured to provide alerts when existing log data or files are changed or deleted. However, new log data being added to an audit log should not generate an alert.

Definitions

Examples

Further Information

sections 10 | top

REQUIREMENTS and TESTING PROCEDURES 10.4

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

DEFINED APPROACH REQUIREMENTS

10.4.1 The following audit logs are reviewed at least once daily:

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).

CUSTOMIZED APPROACH OBJECTIVE

Potentially suspicious or anomalous activities are quickly identified to minimize impact.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.4.1.a Examine security policies and procedures to verify that processes are defined for reviewing all elements specified in this requirement at least once daily.

10.4.1.b Observe processes and interview personnel to verify that all elements specified in this requirement are reviewed at least once daily.

GUIDANCE

Purpose

Many breaches occur months before being detected. Regular log reviews mean incidents can be quickly identified and proactively addressed.

Good Practice

Checking logs daily (7 days a week, 365 days a year, including holidays) minimizes the amount of time and exposure of a potential breach. Log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions are examples of automated tools that can be used to meet this requirement.

Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file integrity monitoring (FIM) systems, etc., is necessary to identify potential issues.

The determination of “security event” will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of “normal” traffic to help identify anomalous behavior. An entity that uses third-party service providers to perform log review services is responsible to provide context about the entity’s environment to the service providers, so it understands the entity’s environment, has a baseline of “normal” traffic for the entity, and can detect potential security issues and provide accurate exceptions and anomaly notifications.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.4.1.1 Automated mechanisms are used to perform audit log reviews.

CUSTOMIZED APPROACH OBJECTIVE

Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

10.4.1.1 Examine log review mechanisms and interview personnel to verify that automated mechanisms are used to perform log reviews.

GUIDANCE

Purpose

Manual log reviews are difficult to perform, even for one or two systems, due to the amount of log data that is generated. However, using log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions can help facilitate the process by identifying log events that need to be reviewed.

Good Practice

The entity should keep logging tools aligned with any changes in their environment by periodically reviewing tool settings and updating settings to reflect any changes.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.

CUSTOMIZED APPROACH OBJECTIVE

Potentially suspicious or anomalous activities for other system components (not included in 10.4.1) are reviewed in accordance with the entity's identified risk.

APPLICABILITY NOTES

This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.

DEFINED APPROACH TESTING PROCEDURES

10.4.2.a Examine security policies and procedures to verify that processes are defined for reviewing logs of all other system components periodically. 10.4.2.b Examine documented results of log reviews and interview personnel to verify that log reviews are performed periodically.

GUIDANCE

Purpose

Periodic review of logs for all other system components (not specified in Requirement 10.4.1) helps to identify indications of potential issues or attempts to access critical systems via less-critical systems.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1

CUSTOMIZED APPROACH OBJECTIVE

Log reviews for lower-risk system components are performed at a frequency that addresses the entity's risk.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

10.4.2.1.a Examine the entity's targeted risk analysis for the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.

10.4.2.1.b Examine documented results of periodic log reviews of all other system components (not defined in Requirement 10.4.1) and interview personnel to verify log

reviews are performed at the frequency specified in the entity's targeted risk analysis performed for this requirement.

GUIDANCE

Purpose

Entities can determine the optimum period to review these logs based on criteria such as the complexity of each entity's environment, the number of types of systems that are required to be evaluated, and the functions of such systems.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.4.3 Exceptions and anomalies identified during the review process are addressed.

CUSTOMIZED APPROACH OBJECTIVE

Suspicious or anomalous activities are addressed.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.4.3.a Examine security policies and procedures to verify that processes are defined for addressing exceptions and anomalies identified during the review process.

10.4.3.b Observe processes and interview personnel to verify that, when exceptions and anomalies are identified, they are addressed.

GUIDANCE

Purpose

If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities occurring within their network.

Good Practice

Entities should consider how to address the following when developing their processes for defining and managing exceptions and anomalies:

- How log review activities are recorded,
- How to rank and prioritize exceptions and anomalies,
- What procedures should be in place to report and escalate exceptions and anomalies, and
- Who is responsible for investigating and for any remediation tasks.

Definitions

Examples

Further Information

sections 10 | top

REQUIREMENTS and TESTING PROCEDURES 10.5

10.5 Audit log history is retained and available for analysis.

DEFINED APPROACH REQUIREMENTS

10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.

CUSTOMIZED APPROACH OBJECTIVE

Historical records of activity are available immediately to support incident response and are retained for at least 12 months.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.5.1.a Examine documentation to verify that the following is defined:

- Audit log retention policies.

- Procedures for retaining audit log history for at least 12 months, with at least the most recent three months immediately available online.

10.5.1.b Examine configurations of audit log history, interview personnel and examine audit logs to verify that audit logs history is retained for at least 12 months.

10.5.1.c Interview personnel and observe processes to verify that at least the most recent three months' audit log history is immediately available for analysis.

GUIDANCE

Purpose

Retaining historical audit logs for at least 12 months is necessary because compromises often go unnoticed for significant lengths of time. Having centrally stored log history allows investigators to better determine the length of time a potential breach was occurring, and the possible system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach.

Good Practice

Definitions

Examples

Methods that allow logs to be immediately available include storing logs online, archiving logs, or restoring logs quickly from backups.

Further Information

sections 10 | top

REQUIREMENTS and TESTING PROCEDURES 10.6

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

DEFINED APPROACH REQUIREMENTS

10.6.1 System clocks and time are synchronized using time-synchronization technology.

CUSTOMIZED APPROACH OBJECTIVE

Common time is established across all systems.

APPLICABILITY NOTES

Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.

DEFINED APPROACH TESTING PROCEDURES

10.6.1 Examine system configuration settings to verify that time-synchronization technology is implemented and kept current.

GUIDANCE

Purpose

Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of events, which is crucial for forensic analysis following a breach.

For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity are critical in determining how the systems were compromised.

Good Practice

Definitions

Examples

Network Time Protocol (NTP) is one example of time-synchronization technology.

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.6.2 Systems are configured to the correct and consistent time as follows:

- One or more designated time servers are in use.
- Only the designated central time server(s) receives time from external sources.
- Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).
- The designated time server(s) accept time updates only from specific industry-accepted external sources.

- Where there is more than one designated time server, the time servers peer with one another to keep accurate time.
- Internal systems receive time information only from designated central time server(s).

CUSTOMIZED APPROACH OBJECTIVE

The time on all systems is accurate and consistent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.6.2 Examine system configuration settings for acquiring, distributing, and storing the correct time to verify the settings are configured in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Using reputable time servers is a critical component of the time synchronization process.

Accepting time updates from specific, industry-accepted external sources helps prevent a malicious individual from changing time settings on systems.

Good Practice

Another option to prevent unauthorized use of internal time servers is to encrypt updates with a symmetric key and create access control lists that specify the IP addresses of client machines that will be provided with the time updates.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.6.3 Time synchronization settings and data are protected as follows:

- Access to time data is restricted to only personnel with a business need.

- Any changes to time settings on critical systems are logged, monitored, and reviewed.

CUSTOMIZED APPROACH OBJECTIVE

System time settings cannot be modified by unauthorized personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

10.6.3.a Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need.

10.6.3.b Examine system configurations and time synchronization settings and logs and observe processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.

GUIDANCE

Purpose

Attackers will try to change time configurations to hide their activity. Therefore, restricting the ability to change or modify time synchronization configurations or the system time to administrators will lessen the probability of an attacker successfully changing time configurations.

Good Practice

Definitions

Examples

Further Information

sections 10 | top

REQUIREMENTS and TESTING PROCEDURES 10.7

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

DEFINED APPROACH REQUIREMENTS

10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

- Network security controls.
- IDS/IPS.
- FIM.
- Anti-malware solutions.
- Physical access controls.
- Logical access controls.
- Audit logging mechanisms.
- Segmentation controls (if used).

CUSTOMIZED APPROACH OBJECTIVE

Failures in critical security control systems are promptly identified and addressed.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement will be superseded by Requirement 10.7.2 as of 31 March 2025.

DEFINED APPROACH TESTING PROCEDURES

10.7.1.a Additional testing procedure for service provider assessments only: Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.

10.7.1.b Additional testing procedure for service provider assessments only: Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.

GUIDANCE

Purpose

Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE.

Good Practice

The specific types of failures may vary, depending on the function of the device system component and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner, such as a firewall erasing all its rules or going offline.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

- Network security controls.
- IDS/IPS.
- Change-detection mechanisms.
- Anti-malware solutions.
- Physical access controls.
- Logical access controls.
- Audit logging mechanisms.
- Segmentation controls (if used).
- Audit log review mechanisms.
- Automated security testing tools (if used).

CUSTOMIZED APPROACH OBJECTIVE

Failures in critical security control systems are promptly identified and addressed.

APPLICABILITY NOTES

This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

10.7.2.a Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.

10.7.2.b Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.

GUIDANCE

Purpose

Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE.

Good Practice

The specific types of failures may vary, depending on the function of the device system component and technology in use. However, typical failures include a system no longer performing its security function or not functioning in its intended manner—for example, a firewall erasing its rules or going offline.

Definitions

Examples

Further Information

sections 10 | top

DEFINED APPROACH REQUIREMENTS

10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to:

- Restoring security functions.

- Identifying and documenting the duration (date and time from start to end) of the security failure.
- Identifying and documenting the cause(s) of failure and documenting required remediation.
- Identifying and addressing any security issues that arose during the failure.
- Determining whether further actions are required as a result of the security failure.
- Implementing controls to prevent the cause of failure from reoccurring.
- Resuming monitoring of security controls.

CUSTOMIZED APPROACH OBJECTIVE

Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities.

This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

10.7.3.a Examine documentation and interview personnel to verify that processes are defined and implemented to respond to a failure of any critical security control system and include at least all elements specified in this requirement.

10.7.3.b Examine records to verify that failures of critical security control systems are documented to include:

- Identification of cause(s) of the failure.
- Duration (date and time start and end) of the security failure.
- Details of the remediation required to address the root cause.

GUIDANCE

Purpose

If alerts from failures of critical security control systems are not responded to quickly and effectively, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment.

Good Practice

Documented evidence (for example, records within a problem management system) should provide support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.

Definitions

Examples

Further Information

sections 10 | top

PRINCIPLE PCI DSS REQUIREMENT: Regularly Monitor and Test Networks

Requirement 11: Test Security of Systems and Networks Regularly

OVERVIEW

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 11

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.6 Unauthorized changes on payment pages are detected and responded to.

requirement 11 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 11.1

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

DEFINED APPROACH REQUIREMENTS

11.1.1 All security policies and operational procedures that are identified in Requirement 11 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

CUSTOMIZED APPROACH OBJECTIVE

Expectations, controls, and oversight for meeting activities within Requirement 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management’s intent.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures are managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Requirement 11.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 11. While it is important to define the specific policies or procedures called out in Requirement 11, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.

CUSTOMIZED APPROACH OBJECTIVE

Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 11 are documented and assigned.

11.1.2.b Interview personnel with responsibility for performing activities in Requirement 11 to verify that roles and responsibilities are assigned as documented and are understood.

GUIDANCE

Purpose

If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.

Good Practice

Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.

As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.

Definitions

Examples

A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).

Further Information

sections 11 | top

REQUIREMENTS and TESTING PROCEDURES 11.2

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

DEFINED APPROACH REQUIREMENTS

11.2.1 Authorized and unauthorized wireless access points are managed as follows:

- The presence of wireless (Wi-Fi) access points is tested for,
- All authorized and unauthorized wireless access points are detected and identified,
- Testing, detection, and identification occurs at least once every three months.
- If automated monitoring is used, personnel are notified via generated alerts.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized wireless access points are identified and addressed periodically.

APPLICABILITY NOTES

The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers do not read and follow company policy.

Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.

DEFINED APPROACH TESTING PROCEDURES

11.2.1.a Examine policies and procedures to verify processes are defined for managing both authorized and unauthorized wireless access points with all elements specified in this requirement.

11.2.1.b Examine the methodology(ies) in use and the resulting documentation, and interview personnel to verify processes are defined to detect and identify both authorized and unauthorized wireless access points in accordance with all elements specified in this requirement.

11.2.1.c Examine wireless assessment results and interview personnel to verify that wireless assessments were conducted in accordance with all elements specified in this requirement.

11.2.1.d If automated monitoring is used, examine configuration settings to verify the configuration will generate alerts to notify personnel.

GUIDANCE

Purpose

Implementation and/or exploitation of wireless technology within a network are common paths for malicious users to gain unauthorized access to the network and cardholder data. Unauthorized wireless devices could be hidden within or attached to a computer or other system component. These devices could also be attached directly to a network port, to a network device such as a switch or router, or inserted as a wireless interface card inside a system component.

If a wireless device or network is installed without a company's knowledge, it can allow an attacker to enter the network easily and "invisibly." Detecting and removing such unauthorized access points reduces the duration and likelihood of such devices being leveraged for an attack.

Good Practice

The size and complexity of an environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment.

For example, performing a detailed physical inspection of a single stand-alone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes (such as in a large retail store, call center, server room or data center), detailed physical inspection can be difficult. In this case, multiple methods may be combined, such as performing physical system inspections in conjunction with the results of a wireless analyzer.

Definitions

This is also referred to as rogue access point detection.

Examples

Methods that may be used include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. NAC and wireless IDS/IPS are examples of automated monitoring tools.

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.

CUSTOMIZED APPROACH OBJECTIVE

Unauthorized wireless access points are not mistaken for authorized wireless access points.

APPLICABILITY NOTES

11.2.2 Examine documentation to verify that an inventory of authorized wireless access points is maintained, and a business justification is documented for all authorized wireless access points.

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

An inventory of authorized wireless access points can help administrators quickly respond when unauthorized wireless access points are detected. This helps to proactively minimize the exposure of CDE to malicious individuals.

Good Practice

If using a wireless scanner, it is equally important to have a defined list of known access points which, while not attached to the company's network, will usually be detected during a scan. These non-company devices are often found in multi-tenant buildings or businesses located near one another. However, it is important to verify that these devices are not connected to the entity's network port or through another network-connected device and given an SSID resembling a nearby business. Scan results should note such devices and how it was determined that these devices could be "ignored." In addition, detection of any unauthorized wireless access points that are determined to be a threat to the CDE should be managed following the entity's incident response plan per Requirement 12.10.1.

Definitions

Examples

Further Information

sections 11 | top

REQUIREMENTS and TESTING PROCEDURES 11.3

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

DEFINED APPROACH REQUIREMENTS

11.3.1 Internal vulnerability scans are performed as follows:

- At least once every three months.
- High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
- Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.
- Scan tool is kept up to date with latest vulnerability information.
- Scans are performed by qualified personnel and organizational independence of the tester exists.

CUSTOMIZED APPROACH OBJECTIVE

The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.

APPLICABILITY NOTES

It is not required to use a QSA or ASV to conduct internal vulnerability scans.

Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.

DEFINED APPROACH TESTING PROCEDURES

11.3.1.a Examine internal scan report results from the last 12 months to verify that internal scans occurred at least once every three months in the most recent 12-month period.

11.3.1.b Examine internal scan report results from each scan and rescan run in the last 12 months to verify that all high-risk and critical vulnerabilities (identified in PCI DSS Requirement 6.3.1) are resolved.

11.3.1.c Examine scan tool configurations and interview personnel to verify that the scan tool is kept up to date with the latest vulnerability information.

11.3.1.d Interview responsible personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and that organizational

independence of the tester exists.

GUIDANCE

Purpose

Identifying and addressing vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or cardholder data. Vulnerability scans conducted at least every three months provide this detection and identification.

Good Practice

Vulnerabilities posing the greatest risk to the environment (for example, ranked high or critical per Requirement 6.3.1) should be resolved with the highest priority.

Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities were resolved as part of the three-month vulnerability scan cycle. However, additional, documentation may be required to verify non-remediated vulnerabilities are in the process of being resolved.

While scans are required at least once every three months, more frequent scans are recommended depending on the network complexity, frequency of change, and types of devices, software, and operating systems used.

Definitions

A vulnerability scan is a combination of automated tools, techniques, and/or methods run against external and internal devices and servers, designed to expose potential vulnerabilities in applications, operating systems, and network devices that could be found and exploited by malicious individuals.

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:

- Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.
- Rescans are conducted as needed.

CUSTOMIZED APPROACH OBJECTIVE

Lower ranked vulnerabilities (lower than high or critical) are addressed at a frequency in accordance with the entity's risk.

APPLICABILITY NOTES

The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

11.3.1.1.a Examine the entity's targeted risk analysis that defines the risk for addressing all other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings at Requirement 6.3.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.

11.3.1.1.b Interview responsible personnel and examine internal scan report results or other documentation to verify that all other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis, and that the scan process includes rescans as needed to confirm the vulnerabilities have been addressed.

GUIDANCE

Purpose

All vulnerabilities, regardless of criticality, provide a potential avenue of attack and must therefore be addressed periodically, with the vulnerabilities that expose the most risk addressed more quickly to limit the potential window of attack.

Good Practice

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows:

- Systems that are unable to accept credentials for authenticated scanning are documented.
- Sufficient privileges are used for those systems that accept credentials for scanning.
- If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.

CUSTOMIZED APPROACH OBJECTIVE

Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely.

APPLICABILITY NOTES

The authenticated scanning tools can be either host-based or network-based. “Sufficient” privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities.

This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

11.3.1.2.a Examine scan tool configurations to verify that authenticated scanning is used for internal scans, with sufficient privileges, for those systems that accept credentials for scanning.

11.3.1.2.b Examine scan report results and interview personnel to verify that authenticated scans are performed.

11.3.1.2.c If accounts used for authenticated scanning can be used for interactive login, examine the accounts and interview personnel to verify the accounts are managed following all elements specified in Requirement 8.2.2.

11.3.1.2.d Examine documentation to verify that systems that are unable to accept credentials for authenticated scanning are defined.

GUIDANCE

Purpose

Authenticated scanning provides greater insight into an entity's vulnerability landscape since it can detect vulnerabilities that unauthenticated scans cannot detect. Attackers may leverage vulnerabilities that an entity is unaware of because certain vulnerabilities will only be detected with authenticated scanning.

Authenticated scanning can yield significant additional information about an organization's vulnerabilities.

Good Practice

The credentials used for these scans should be considered highly privileged. They should be protected and controlled as such, following PCI DSS Requirements 7 and 8 (except for those requirements for multi-factor authentication and application and system accounts).

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.3.1.3 Internal vulnerability scans are performed after any significant change as follows:

- High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.
- Rescans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

CUSTOMIZED APPROACH OBJECTIVE

The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.

APPLICABILITY NOTES

Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.

DEFINED APPROACH TESTING PROCEDURES

11.3.1.3.a Examine change control documentation and internal scan reports to verify that system components were scanned after any significant changes.

11.3.1.3.b Interview personnel and examine internal scan and rescan reports to verify that internal scans were performed after significant changes and that high-risk and critical vulnerabilities as defined in Requirement 6.3.1 were resolved.

11.3.1.3.c Interview personnel to verify that internal scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.

GUIDANCE

Purpose

Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change.

Good Practice

Entities should perform scans after significant changes as part of the change process per Requirement 6.5.2 and before considering the change complete. All system components affected by the change will need to be scanned.

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.3.2 External vulnerability scans are performed as follows:

- At least once every three months.
- By a PCI SSC Approved Scanning Vendor (ASV).
- Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
- Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).

However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred.

ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer.

Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.

DEFINED APPROACH TESTING PROCEDURES

11.3.2.a Examine ASV scan reports from the last 12 months to verify that external vulnerability scans occurred at least once every three months in the most recent 12-month period.

11.3.2.b Examine the ASV scan report from each scan and rescan run in the last 12 months to verify that vulnerabilities are resolved and the ASV Program Guide requirements for a

passing scan are met.

11.3.2.c Examine the ASV scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).

GUIDANCE

Purpose

Attackers routinely look for unpatched or vulnerable externally facing servers, which can be leveraged to launch a directed attack. Organizations must ensure these externally facing devices are regularly scanned for weaknesses and that vulnerabilities are patched or remediated to protect the entity.

Because external networks are at greater risk of compromise, external vulnerability scanning must be performed at least once every three months by a PCI SSC Approved Scanning Vendor (ASV).

Good Practice

While scans are required at least once every three months, more frequent scans are recommended depending on the network complexity, frequency of change, and types of devices, software, and operating systems used.

Multiple scan reports can be combined to show that all systems were scanned and that all applicable vulnerabilities were resolved as part of the three-month vulnerability scan cycle. However, additional documentation may be required to verify non-remediated vulnerabilities are in the process of being resolved.

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.3.2.1 External vulnerability scans are performed after any significant change as follows:

- Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
- Rescans are conducted as needed.

- Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

CUSTOMIZED APPROACH OBJECTIVE

The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.3.2.1.a Examine change control documentation and external scan reports to verify that system components were scanned after any significant changes.

11.3.2.1.b Interview personnel and examine external scan and rescan reports to verify that external scans were performed after significant changes and that vulnerabilities scored 4.0 or higher by the CVSS were resolved.

11.3.2.1.c Interview personnel to verify that external scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.

GUIDANCE

Purpose

Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change.

Good Practice

Entities should include the need to perform scans after significant changes as part of the change process and before the change is considered complete. All system components affected by the change will need to be scanned.

Definitions

Examples

Further Information

REQUIREMENTS and TESTING PROCEDURES 11.4

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

DEFINED APPROACH REQUIREMENTS

11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes:

- Industry-accepted penetration testing approaches.
- Coverage for the entire CDE perimeter and critical systems.
- Testing from both inside and outside the network.
- Testing to validate any segmentation and scope-reduction controls.
- Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.
- Network-layer penetration tests that encompass all components that support network functions as well as operating systems.
- Review and consideration of threats and vulnerabilities experienced in the last 12 months.
- Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.
- Retention of penetration testing results and remediation activities results for at least 12 months.

CUSTOMIZED APPROACH OBJECTIVE

A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.

APPLICABILITY NOTES

Testing from inside the network (or “internal penetration testing”) means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks.

Testing from outside the network (or “external penetration testing”) means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.

11.4.1 Examine documentation and interview personnel to verify that the penetration-testing methodology defined, documented, and implemented by the entity includes all elements specified in this requirement.

GUIDANCE

Purpose

Attackers spend a lot of time finding external and internal vulnerabilities to leverage to obtain access to cardholder data and then to exfiltrate that data. As such, entities need to test their networks thoroughly, just as an attacker would do. This testing allows the entity to identify and remediate weakness that might be leveraged to compromise the entity's network and data, and then to take appropriate actions to protect the network and system components from such attacks.

Good Practice

Penetration testing techniques will differ based on an organization's needs and structure and should be suitable for the tested environment—for example, fuzzing, injection, and forgery tests might be appropriate. The type, depth, and complexity of the testing will depend on the specific environment and the needs of the organization.

Definitions

Penetration tests simulate a real-world attack situation intending to identify how far an attacker could penetrate an environment, given differing amounts of information provided to the tester. This allows an entity to better understand its potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that usually includes exploiting identified vulnerabilities.

Scanning for vulnerabilities alone is not a penetration test, nor is a penetration test adequate if the focus is solely on trying to exploit vulnerabilities found in a vulnerability scan. Conducting a vulnerability scan may be one of the first steps, but it is not the only step a penetration tester will perform to plan the testing strategy. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps.

Penetration testing is a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to gain access into an environment. Often the tester will chain several types of exploits together with the goal of breaking through layers

of defenses. For example, if the tester finds a way to gain access to an application server, the tester will then use the compromised server as a point to stage a new attack based on the resources to which the server has access. In this way, a tester can simulate the techniques used by an attacker to identify areas of potential weakness in the environment. The testing of security monitoring and detection methods—for example, to confirm the effectiveness of logging and file integrity monitoring mechanisms, should also be considered.

Examples

Further Information

Refer to the *Information Supplement: Penetration Testing Guidance* for additional guidance. Industry-accepted penetration testing approaches include: *The Open Source Security Testing Methodology and Manual (OSSTMM) Open Web Application Security Project (OWASP) penetration testing programs*.

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.4.2 Internal penetration testing is performed:

- Per the entity's defined methodology,
- At least once every 12 months
- After any significant infrastructure or application upgrade or change
- By a qualified internal resource or qualified external third-party
- Organizational independence of the tester exists (not required to be a QSA or ASV).

CUSTOMIZED APPROACH OBJECTIVE

Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.4.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed in accordance with all elements specified in this requirement.

11.4.2.b Interview personnel to verify that the internal penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).

GUIDANCE

Purpose

Purpose Internal penetration testing serves two purposes. Firstly, just like an external penetration test, it discovers vulnerabilities and misconfigurations that could be used by an attacker that had managed to get some degree of access to the internal network, whether that is because the attacker is an authorized user conducting unauthorized activities, or an external attacker that had managed to penetrate the entity's perimeter.

Secondly, internal penetration testing also helps entities to discover where their change control process failed by detecting previously unknown systems. Additionally, it verifies the status of many of the controls operating within the CDE.

A penetration test is not truly a "test" because the outcome of a penetration test is not something that can be classified as a "pass" or a "fail." The best outcome of a test is a catalog of vulnerabilities and misconfigurations that an entity did not know about and the penetration tester found them before an attacker could. A penetration test that found nothing is typically indicative of shortcomings of the penetration tester, rather than being a positive reflection of the security posture of the entity.

Good Practice

Some considerations when choosing a qualified resource to perform penetration testing include:

- Specific penetration testing certifications, which may be an indication of the tester's skill level and competence.
- Prior experience conducting penetration testing—for example, the number of years of experience, and the type and scope of prior engagements can help confirm whether the tester's experience is appropriate for the needs of the engagement.

Definitions

Examples

Further Information

Refer to the *Information Supplement: Penetration Testing Guidance* on the PCI SSC website for additional guidance.

DEFINED APPROACH REQUIREMENTS

11.4.3 External penetration testing is performed:

- Per the entity's defined methodology
- At least once every 12 months
- After any significant infrastructure or application upgrade or change
- By a qualified internal resource or qualified external third party
- Organizational independence of the tester exists (not required to be a QSA or ASV).

CUSTOMIZED APPROACH OBJECTIVE

External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown vulnerabilities.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.4.3.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed according to all elements specified in this requirement.

11.4.3.b Interview personnel to verify that the external penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).

GUIDANCE

Purpose

Purpose Internal penetration testing serves two purposes. Firstly, just like an external penetration test, it discovers vulnerabilities and misconfigurations that could be used by an attacker that had managed to get some degree of access to the internal network, whether that is because the attacker is an authorized user conducting unauthorized activities, or an external attacker that had managed to penetrate the entity's perimeter.

Secondly, internal penetration testing also helps entities to discover where their change control process failed by detecting previously unknown systems. Additionally, it verifies the

status of many of the controls operating within the CDE.

A penetration test is not truly a “test” because the outcome of a penetration test is not something that can be classified as a “pass” or a “fail.” The best outcome of a test is a catalog of vulnerabilities and misconfigurations that an entity did not know about and the penetration tester found them before an attacker could. A penetration test that found nothing is typically indicative of shortcomings of the penetration tester, rather than being a positive reflection of the security posture of the entity.

Good Practice

Some considerations when choosing a qualified resource to perform penetration testing include:

- Specific penetration testing certifications, which may be an indication of the tester’s skill level and competence.
- Prior experience conducting penetration testing—for example, the number of years of experience, and the type and scope of prior engagements can help confirm whether the tester’s experience is appropriate for the needs of the engagement.

Definitions

Examples

Further Information

Refer to the *Information Supplement: Penetration Testing Guidance* on the PCI SSC website for additional guidance.

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:

- In accordance with the entity’s assessment of the risk posed by the security issue as defined in Requirement 6.3.1.
- Penetration testing is repeated to verify the corrections.

CUSTOMIZED APPROACH OBJECTIVE

Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.4.4 Examine penetration testing results to verify that noted exploitable vulnerabilities and security weaknesses were corrected in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

The results of a penetration test are usually a prioritized list of vulnerabilities discovered by the exercise. Often a tester will have chained a number of vulnerabilities together to compromise a system component. Remediating the vulnerabilities found by a penetration test significantly reduces the probability that the same vulnerabilities will be exploited by a malicious attacker.

Using the entity's own vulnerability risk assessment process (see requirement 6.3.1) ensures that the vulnerabilities that pose the highest risk to the entity will be remediated more quickly.

Good Practice

As part of the entity's assessment of risk, entities should consider how likely the vulnerability is to be exploited and whether there are other controls present in the environment to reduce the risk.

Any weaknesses that point to PCI DSS requirements not being met should be addressed.

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

- At least once every 12 months and after any changes to segmentation controls/methods
- Covering all segmentation controls/methods in use.
- According to the entity's defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

CUSTOMIZED APPROACH OBJECTIVE

If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out-of-scope systems.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.4.5.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods in accordance with all elements specified in this requirement.

11.4.5.b Examine the results from the most recent penetration test to verify the penetration test covers and addresses all elements specified in this requirement.

11.4.5.c Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).

GUIDANCE

Purpose

When an entity uses segmentation controls to isolate the CDE from internal untrusted networks, the security of the CDE is dependent on that segmentation functioning. Many attacks have involved the attacker moving laterally from what an entity deemed an isolated network into the CDE. Using penetration testing tools and techniques to validate that an

untrusted network is indeed isolated from the CDE can alert the entity to a failure or misconfiguration of the segmentation controls, which can then be rectified.

Good Practice

Techniques such as host discovery and port scanning can be used to verify out-of-scope segments have no access to the CDE.

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

- At least once every six months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- According to the entity's defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

CUSTOMIZED APPROACH OBJECTIVE

If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

11.4.6.a Additional testing procedure for service provider assessments only: Examine the results from the most recent penetration test to verify that the penetration covers and addressed all elements specified in this requirement.

11.4.6.b Additional testing procedure for service provider assessments only: Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).

GUIDANCE

Purpose

Service providers typically have access to greater volumes of cardholder data or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of segmentation controls failing in complex and dynamic networks is greater in service provider environments.

Validating segmentation controls more frequently is likely to discover such failings before they can be exploited by an attacker attempting to pivot laterally from an out-of-scope untrusted network to the CDE.

Good Practice

Although the requirement specifies that this scope validation is carried out at least once every six months and after significant change, this exercise should be performed as frequently as possible to ensure it remains effective at isolating the CDE from other networks.

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.4.7 Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.

CUSTOMIZED APPROACH OBJECTIVE

Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a multi-tenant service provider. To meet this requirement, a multi-tenant service provider may either:

- Provide evidence to its customers to show that penetration testing has been performed according to Requirements 11.4.3 and 11.4.4 on the customers' subscribed infrastructure, or
- Provide prompt access to each of its customers, so customers can perform their own penetration testing. Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Requirements 11.4.3 and 11.4.4 have been met on the customer's behalf. Refer also to Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

11.4.7 Additional testing procedure for multi-tenant service providers only: Examine evidence to verify that multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.

GUIDANCE

Purpose

Entities need to conduct penetration tests in accordance with PCI DSS to simulate attacker behavior and discover vulnerabilities in their environment. In shared and cloud environments, the multi-tenant service provider may be concerned about the activities of a penetration tester affecting other customers' systems.

Multi-tenant service providers cannot forbid penetration testing because this would leave their customers' systems open to exploitation. Therefore, multi-tenant service providers must support customer requests to conduct penetration testing or for penetration testing results.

Good Practice

Definitions

Examples

Further Information

sections 11 | top

REQUIREMENTS and TESTING PROCEDURES 11.5

11.5 Network intrusions and unexpected file changes are detected and responded to.

DEFINED APPROACH REQUIREMENTS

11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows:

- All traffic is monitored at the perimeter of the CDE.
- All traffic is monitored at critical points in the CDE.
- Personnel are alerted to suspected compromises.
- All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.

CUSTOMIZED APPROACH OBJECTIVE

Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

11.5.1.a Examine system configurations and network diagrams to verify that intrusion-detection and/or intrusion-prevention techniques are in place to monitor all traffic:

- At the perimeter of the CDE.
- At critical points in the CDE.

11.5.1.b Examine system configurations and interview responsible personnel to verify intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.

11.5.1.c Examine system configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured to keep all engines, baselines, and signatures up to date.

GUIDANCE

Purpose

Intrusion-detection and/or intrusion-prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and then send alerts and/or stop the attempt as it happens. Without a proactive approach to detect unauthorized activity, attacks on (or misuse of) computer resources could go unnoticed for long periods of time. The impact of an intrusion into the CDE is, in many ways, a factor of the time that an attacker has in the environment before being detected.

Good Practice

Security alerts generated by these techniques should be continually monitored, so that the attempted or actual intrusions can be stopped, and potential damage limited.

Definitions

Critical locations could include, but are not limited to, network security controls between network segments (for example, between a DMZ and an internal network or between an in-scope and out-of-scope network) and points protecting connections between a less trusted and a more trusted system component.

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.5.1.1 Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.

CUSTOMIZED APPROACH OBJECTIVE

Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

11.5.1.1.a Additional testing procedure for service provider assessments only: Examine documentation and configuration settings to verify that methods to detect and alert on/prevent covert malware communication channels are in place and operating.

11.5.1.1.b Additional testing procedure for service provider assessments only: Examine the entity's incident-response plan (Requirement 12.10.1) to verify it requires and defines a response in the event that covert malware communication channels are detected.

11.5.1.1.c Additional testing procedure for service provider assessments only: Interview responsible personnel and observe processes to verify that personnel maintain knowledge of covert malware communication and control techniques and are knowledgeable about how to respond when malware is suspected.

GUIDANCE

Purpose

Detecting covert malware communication attempts (for example, DNS tunneling) can help block the spread of malware laterally inside a network and the exfiltration of data. When deciding where to place this control, entities should consider critical locations in the network, and likely routes for covert channels.

When malware establishes a foothold in an infected environment, it often tries to establish a communication channel to a command-and-control (C&C) server. Through the C&C server, the attacker communicates with and controls malware on compromised systems to deliver malicious payloads or instructions, or to initiate data exfiltration. In many cases, the malware will communicate with the C&C server indirectly via botnets, bypassing monitoring, blocking controls, and rendering these methods ineffective to detect the covert channels.

Good Practice

Methods that can help detect and address malware communications channels include real-time endpoint scanning, egress traffic filtering, an ”allow” listing, data loss prevention tools, and network security monitoring tools such as IDS/IPS. Additionally, DNS queries and responses are a key data source used by network defenders in support of incident response as well as intrusion discovery. When these transactions are collected for processing and analytics, they can enable a number of valuable security analytic scenarios.

It is important that organizations maintain up-to-date knowledge of malware modes of operation, as mitigating these can help detect and limit the impact of malware in the environment.

Definitions

Examples

Further Information

sections 11 | top

DEFINED APPROACH REQUIREMENTS

11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:

- To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.
- To perform critical file comparisons at least once weekly.

CUSTOMIZED APPROACH OBJECTIVE

Critical files cannot be modified by unauthorized personnel without an alert being generated.

APPLICABILITY NOTES

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

DEFINED APPROACH TESTING PROCEDURES

11.5.2.a Examine system settings, monitored files, and results from monitoring activities to verify the use of a change-detection mechanism.

11.5.2.b Examine settings for the change-detection mechanism to verify it is configured in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Changes to critical system, configuration, or content files can be an indicator an attacker has accessed an organization's system. Such changes can allow an attacker to take additional malicious actions, access cardholder data, and/or conduct activities without detection or record.

A change detection mechanism will detect and evaluate such changes to critical files and generate alerts that can be responded to following defined processes so that personnel can take appropriate actions.

If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.

Good Practice

Examples of the types of files that should be monitored include, but are not limited to:

- System executables.
- Application executables.
- Configuration and parameter files.
- Centrally stored, historical, or archived audit logs.
- Additional critical files determined by entity (for example, through risk assessment or other means).

Definitions

Examples

Change-detection solutions such as file integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected.

Further Information

sections 11 | top

REQUIREMENTS and TESTING PROCEDURES 11.6

11.6 Unauthorized changes on payment pages are detected and responded to.

DEFINED APPROACH REQUIREMENTS

11.6.1 A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP header and payment page.
- The mechanism functions are performed as follows:
- At least once every seven days

OR

- Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).

CUSTOMIZED APPROACH OBJECTIVE

E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.

APPLICABILITY NOTES

The intention of this requirement is not that an entity installs software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the Guidance column to prevent and detect unexpected script activities.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

11.6.1.a Examine system settings, monitored payment pages, and results from monitoring activities to verify the use of a change- and tamper-detection mechanism.

11.6.1.b Examine configuration settings to verify the mechanism is configured in accordance with all elements specified in this requirement.

11.6.1.c If the mechanism functions are performed at an entity-defined frequency, examine the entity's targeted risk analysis for determining the frequency to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.

11.6.1.d Examine configuration settings and interview personnel to verify the mechanism functions are performed either:

- At least once every seven days

OR

- At the frequency defined in the entity's targeted risk analysis performed for this requirement.

GUIDANCE

Purpose

Many web pages now rely on assembling objects, including active content (primarily JavaScript), from multiple internet locations. Additionally, the content of many web pages is defined using content management and tag management systems that may not be possible to monitor using traditional change detection mechanisms.

Therefore, the only place to detect changes or indicators of malicious activity is in the consumer browser as the page is constructed and all JavaScript interpreted.

By comparing the current version of the HTTP header and the active content of payment pages as received by the consumer browser with prior or known versions, it is possible to detect unauthorized changes that may indicate a skimming attack.

Additionally, by looking for known indicators of compromise and script elements or behavior typical of skimmers, suspicious alerts can be raised.

Good Practice

Definitions

Examples

Mechanisms that detect and report on changes to the headers and content of the payment page include but are not limited to:

- Violations of the Content Security Policy (CSP) can be reported to the entity using the report-to or report-uri CSP directives.
- Changes to the CSP itself can indicate tampering.
- External monitoring by systems that request and analyze the received web pages (also known as synthetic user monitoring) can detect changes to JavaScript in payment pages and alert personnel.
- Embedding tamper-resistant, tamper-detection script in the payment page can alert and block when malicious script behavior is detected.
- Reverse proxies and Content Delivery Networks can detect changes in scripts and alert personnel. Often, these mechanisms are subscription or cloud-based, but can also be based on custom and bespoke solutions.

Further Information

sections 11 | top

PRINCIPLE PCI DSS REQUIREMENT: Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

OVERVIEW

The organization's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of account data.

Refer to Appendix G for definitions of PCI DSS terms.

SECTIONS 12

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.9 Third-party service providers (TPSPs) support their customers’ PCI DSS compliance.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

requirement 12 | requirements | principles | top

REQUIREMENTS and TESTING PROCEDURES 12.1

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current.

DEFINED APPROACH REQUIREMENTS

12.1.1 An overall information security policy is:

- Established.
- Published.
- Maintained.
- Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

CUSTOMIZED APPROACH OBJECTIVE

The strategic objectives and principles of information security are defined, adopted, and known to all personnel.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.1.1 Examine the information security policy and interview personnel to verify that the overall information security policy is managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

An organization’s overall information security policy ties to and governs all other policies and procedures that define protection of cardholder data.

The information security policy communicates management’s intent and objectives regarding the protection of its most valuable assets, including cardholder data.

Without an information security policy, individuals will make their own value decisions on the controls that are required within the organization which may result in the organization neither meeting its legal, regulatory, and contractual obligations, nor being able to adequately protect its assets in a consistent manner.

To ensure the policy is implemented, it is important that all relevant personnel within the organization, as well as relevant third parties, vendors, and business partners are aware of the organization’s information security policy and their responsibilities for protecting information assets.

Good Practice

The security policy for the organization identifies the purpose, scope, accountability, and information that clearly defines the organization’s position regarding information security.

The overall information security policy differs from individual security policies that address specific technology or security disciplines. This policy sets forth the directives for the entire organization whereas individual security policies align and support the overall security policy and communicate specific objectives for technology or security disciplines.

It is important that all relevant personnel within the organization, as well as relevant third parties, vendors, and business partners are aware of the organization’s information security policy and their responsibilities for protecting information assets.

Definitions

“Relevant” for this requirement means that the information security policy is disseminated to those with roles applicable to some or all the topics in the policy, either within the company or because of services/functions performed by a vendor or third party.

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.1.2 The information security policy is:

- Reviewed at least once every 12 months.
- Updated as needed to reflect changes to business objectives or risks to the environment.

CUSTOMIZED APPROACH OBJECTIVE

The information security policy continues to reflect the organization’s strategic objectives and principles.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.1.2 Examine the information security policy and interview responsible personnel to verify the policy is managed in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Security threats and associated protection methods evolve rapidly. Without updating the information security policy to reflect relevant changes, new measures to defend against these threats may not be addressed.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.

CUSTOMIZED APPROACH OBJECTIVE

Personnel understand their role in protecting the entity's cardholder data.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.1.3.a Examine the information security policy to verify that they clearly define information security roles and responsibilities for all personnel.

12.1.3.b Interview personnel in various roles to verify they understand their information security responsibilities.

12.1.3.c Examine documented evidence to verify personnel acknowledge their information security responsibilities.

GUIDANCE

Purpose

Without clearly defined security roles and responsibilities assigned, there could be misuse of the organization's information assets or inconsistent interaction with information security personnel, leading to insecure implementation of technologies or use of outdated or insecure technologies.

Good Practice

Definitions

Examples

Further Information

DEFINED APPROACH REQUIREMENTS

12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.

CUSTOMIZED APPROACH OBJECTIVE

A designated member of executive management is responsible for information security.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.1.4 Examine the information security policy to verify that information security is formally assigned to a Chief Information Security Officer or other information security-knowledgeable member of executive management.

GUIDANCE

Purpose

To ensure someone with sufficient authority and responsibility is actively managing and championing the organization's information security program, accountability and responsibility for information security needs to be assigned at the executive level within an organization.

Common executive management titles for this role include Chief Information Security Officer (CISO) and Chief Security Officer (CSO – to meet this requirement, the CSO role must be responsible for information security). These positions are often at the most senior level of management and are part of the chief executive level or C-level, typically reporting to the Chief Executive Officer or the Board of Directors.

Good Practice

Entities should also consider transition and/or succession plans for these key personnel to avoid potential gaps in critical security activities.

Definitions

Examples

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.2

12.2 Acceptable use policies for end-user technologies are defined and implemented.

DEFINED APPROACH REQUIREMENTS

12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including:

- Explicit approval by authorized parties.
- Acceptable uses of the technology.
- List of products approved by the company for employee use, including hardware and software.

CUSTOMIZED APPROACH OBJECTIVE

The use of end-user technologies is defined and managed to ensure authorized usage.

APPLICABILITY NOTES

Examples of end-user technologies for which acceptable use policies are expected include, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, email usage, and Internet usage.

DEFINED APPROACH TESTING PROCEDURES

12.2.1 Examine the acceptable use policies for end-user technologies and interview responsible personnel to verify processes are documented and implemented in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

End-user technologies are a significant investment and may pose significant risk to an organization if not managed properly. Acceptable use policies outline the expected behavior from personnel when using the organization’s information technology and reflect the organization’s risk tolerance.

These policies instruct personnel on what they can and cannot do with company equipment and instruct personnel on correct and incorrect uses of company Internet and email resources. Such policies can legally protect an organization and allow it to act when the policies are violated.

Good Practice

It is important that usage policies are supported by technical controls to manage the enforcement of the policies.

Structuring polices as simple “do” and “do not” requirements that are linked to a purpose can help remove ambiguity and provide personnel with the context for the requirement.

Definitions

Examples

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.3

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

DEFINED APPROACH REQUIREMENTS

12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.

CUSTOMIZED APPROACH OBJECTIVE

Up to date knowledge and assessment of risks to the CDE are maintained.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.3.1 Examine documented policies and procedures to verify a process is defined for performing targeted risk analyses for each PCI DSS requirement that provides flexibility for how frequently the requirement is performed, and that the process includes all elements specified in this requirement.

GUIDANCE

Purpose

Some PCI DSS requirements allow an entity to define how frequently an activity is performed based on the risk to environment. Performing this risk analysis according to a methodology ensures validity and consistency with policies and procedures.

This targeted risk analysis (as opposed to a traditional enterprise-wide risk assessment) focuses on those PCI DSS requirements that allow an entity flexibility about how frequently an entity performs a given control. For this risk analysis, the entity carefully evaluates each PCI DSS requirement that provides this flexibility and determines the frequency that supports adequate security for the entity, and the level of risk the entity is willing to accept.

The risk analysis identifies the specific assets, such as the system components and data—for example, log files, or credentials—that the requirement is intended to protect, as well as the threat(s) or outcomes that the requirement is protecting the assets from—for example, malware, an undetected intruder, or misuse of credentials. Examples of factors that could contribute to likelihood or impact include any that could increase the vulnerability of an asset to a threat—for example, exposure to untrusted networks, complexity of environment, or high staff turnover—as well as the criticality of the system components, or volume and sensitivity of the data, being protected.

Reviewing the results of these targeted risk analyses at least once every 12 months and upon changes that could impact the risk to the environment allows the organization to ensure the risk analysis results remain current with organizational changes and evolving

threats, trends, and technologies, and that the selected frequencies still adequately address the entity's risk.

Good Practice

An enterprise-wide risk assessment, which is a point-in-time activity that enables entities to identify threats and associated vulnerabilities, is recommended, but is not required, for entities to determine and understand broader and emerging threats with the potential to negatively impact its business. This enterprise-wide risk assessment could be established as part of an overarching risk management program that is used as an input to the annual review of an organization's overall information security policy (see Requirement 12.1.1).

Examples of risk-assessment methodologies for enterprise-wide risk assessments include, but are not limited to, ISO 27005 and NIST *SP 800-30*.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include:

- Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis).
- Approval of documented evidence by senior management.
- Performance of the targeted analysis of risk at least once every 12 months.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is part of the customized approach and must be met for those using the customized approach.

APPLICABILITY NOTES

This requirement only applies to entities using a Customized Approach.

DEFINED APPROACH TESTING PROCEDURES

12.3.2 Examine the documented targeted risk-analysis for each PCI DSS requirement that the entity meets with the customized approach to verify that documentation for each requirement exists and is in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

A risk analysis following a repeatable and robust methodology enables an entity to meet the customized approach objective.

Good Practice

Definitions

The customized approach to meeting a PCI DSS requirement allows entities to define the controls used to meet a given requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. These controls are expected to at least meet or exceed the security provided by the defined requirement and require extensive documentation by the entity using the customized approach.

Examples

Further Information

See Appendix D: Customized Approach for instructions on how to document the required evidence for the customized approach.

See Appendix E Sample Templates to Support Customized Approach for templates that entities may use to document their customized controls. Note that while use of the templates is optional, the information specified within each template must be documented and provided to each entity's assessor.

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:

- An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used.

- Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use.
- A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.

CUSTOMIZED APPROACH OBJECTIVE

The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.

APPLICABILITY NOTES

The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.3.3 Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations.

Good Practice

Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, it can make proactive plans to upgrade before the deprecation is impactful to operations.

Definitions

“Cryptographic agility” refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization.

Examples

Further Information

Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:

- Analysis that the technologies continue to receive security fixes from vendors promptly.
- Analysis that the technologies continue to support (and do not preclude) the entity’s PCI DSS compliance.
- Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced “end of life” plans for a technology.
- Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced “end of life” plans.

CUSTOMIZED APPROACH OBJECTIVE

The entity’s hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.3.4 Examine documentation for the review of hardware and software technologies in use and interview personnel to verify that the review is in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies to ensure that they can prepare for, and manage, vulnerabilities in hardware and software that will not be remediated by the vendor or developer.

Good Practice

Organizations should review firmware versions to ensure they remain current and supported by the vendors. Organizations also need to be aware of changes made by technology vendors to their products or processes to understand how such changes may impact the organization's use of the technology.

Regular reviews of technologies that impact or influence PCI DSS controls can assist with purchasing, usage, and deployment strategies, and ensure controls that rely on those technologies remain effective. These reviews include, but are not limited to, reviewing technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.

Definitions

Examples

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.4

12.4 PCI DSS compliance is managed.

DEFINED APPROACH REQUIREMENTS

12.4.1 Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include:

- Overall accountability for maintaining PCI DSS compliance.
- Defining a charter for a PCI DSS compliance program and communication to executive management.

CUSTOMIZED APPROACH OBJECTIVE

Executives are responsible and accountable for security of cardholder data.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure.

Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.

DEFINED APPROACH TESTING PROCEDURES

12.4.1 Additional testing procedure for service provider assessments only: Examine documentation to verify that executive management has established responsibility for the protection of cardholder data and a PCI DSS compliance program in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.4.2 Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in

accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks:

- Daily log reviews.
- Configuration reviews for network security controls.
- Applying configuration standards to new systems.
- Responding to security alerts.
- Change-management processes.

CUSTOMIZED APPROACH OBJECTIVE

The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

12.4.2.a Additional testing procedure for service provider assessments only: Examine policies and procedures to verify that processes are defined for conducting reviews to confirm that personnel are performing their tasks in accordance with all security policies and all operational procedures, including but not limited to the tasks specified in this requirement.

12.4.2.b Additional testing procedure for service provider assessments only: Interview responsible personnel and examine records of reviews to verify that reviews are performed:

- At least once every three months.
- By personnel other than those responsible for performing the given task.

GUIDANCE

Purpose

Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. This requirement is distinct from other requirements that specify a task to be performed. The objective of

these reviews is not to reperform other PCI DSS requirements, but to confirm that security activities are being performed on an ongoing basis.

Good Practice

These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment.

Definitions

Examples

Looking at Requirement 1.2.7 as one example, Requirement 12.4.2 is met by confirming, at least once every three months, that reviews of configurations of network security controls have occurred at the required frequency. On the other hand, Requirement 1.2.7 is met by reviewing those configurations as specified in the requirement.

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.4.2.1 Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include:

- Results of the reviews.
- Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2.
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

CUSTOMIZED APPROACH OBJECTIVE

Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

12.4.2.1 Additional testing procedure for service provider assessments only: Examine documentation from the reviews conducted in accordance with PCI DSS Requirement 12.4.2 to verify the documentation includes all elements specified in this requirement.

GUIDANCE

Purpose

The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.5

12.5 PCI DSS scope is documented and validated.

DEFINED APPROACH REQUIREMENTS

12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.

CUSTOMIZED APPROACH OBJECTIVE

All system components in scope for PCI DSS are identified and known.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.5.1.a Examine the inventory to verify it includes all in-scope system components and a description of function/use for each.

12.5.1.b Interview personnel to verify the inventory is kept current.

GUIDANCE

Purpose

Maintaining a current list of all system components will enable an organization to define the scope of its environment and implement PCI DSS requirements accurately and efficiently. Without an inventory, some system components could be overlooked and be inadvertently excluded from the organization's configuration standards.

Good Practice

If an entity keeps an inventory of all assets, those system components in scope for PCI DSS should be clearly identifiable among the other assets. Inventories should include containers or images that may be instantiated.

Assigning an owner to the inventory helps to ensure the inventory stays current.

Definitions

Examples

Methods to maintain an inventory include as a database, as a series of files, or in an inventory-management tool.

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:

- Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).
- Updating all data-flow diagrams per Requirement 1.2.4.
- Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2)

applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.
- Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.
- Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.
- Identifying all connections from third-party entities with access to the CDE.
- Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

CUSTOMIZED APPROACH OBJECTIVE

PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.

APPLICABILITY NOTES

This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.

DEFINED APPROACH TESTING PROCEDURES

12.5.2.a Examine documented results of scope reviews and interview personnel to verify that the reviews are performed:

- At least once every 12 months.
- After significant changes to the in-scope environment.

12.5.2.b Examine documented results of scope reviews performed by the entity to verify that PCI DSS scoping confirmation activity includes all elements specified in this requirement.

GUIDANCE

Purpose

Frequent validation of PCI DSS scope helps to ensure PCI DSS scope remains up to date and aligned with changing business objectives, and therefore that security controls are protecting all appropriate system components.

Good Practice

Accurate scoping involves critically evaluating the CDE and all connected system components to determine the necessary coverage for PCI DSS requirements. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information:

- Data stores (databases, files, cloud, etc.), including the purpose of data storage and the retention period,
- Which CHD elements are stored (PAN, expiry date, cardholder name, and/or any elements of SAD prior to completion of authorization),
- How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization),
- How access to data stores is logged, including a description of logging mechanism(s) in use (enterprise solution, application level, operating system level, etc.).

In addition to internal systems and networks, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls can be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE.

A data discovery tool or methodology can be used to facilitate identifying all sources and locations of PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file. This approach can help ensure that previously unknown locations of PAN are detected and that the PAN is either eliminated or properly secured.

Definitions

Examples

Further Information

For additional guidance, refer to *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation*.

sections 12 | top

12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.

CUSTOMIZED APPROACH OBJECTIVE

The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.5.2.1.a Additional testing procedure for service provider assessments only: Examine documented results of scope reviews and interview personnel to verify that reviews per Requirement 12.5.2 are performed:

- At least once every six months, and
- After significant changes

12.5.2.1.b Additional testing procedure for service provider assessments only: Examine documented results of scope reviews to verify that scoping validation includes all elements specified in Requirement 12.5.2.

GUIDANCE

Purpose

Service providers typically have access to greater volumes of cardholder data than do merchants, or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of overlooked changes to scope in complex and dynamic networks is greater in service providers' environments.

Validating PCI DSS scope more frequently is likely to discover such overlooked changes before they can be exploited by an attacker.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.5.3 Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.

CUSTOMIZED APPROACH OBJECTIVE

PCI DSS scope is confirmed after significant organizational change.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.5.3.a Additional testing procedure for service provider assessments only: Examine policies and procedures to verify that processes are defined such that a significant change to organizational structure results in documented review of the impact to PCI DSS scope and applicability of controls.

12.5.3.b Additional testing procedure for service provider assessments only: Examine documentation (for example, meeting minutes) and interview responsible personnel to verify that significant changes to organizational structure resulted in documented reviews that included all elements specified in this requirement, with results communicated to executive management.

GUIDANCE

Purpose

An organization’s structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported PCI DSS controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit PCI DSS scope and controls when there are changes to an organization’s structure and management to ensure controls are in place and active.

Good Practice

Changes to organizational structure include, but are not limited to, company mergers or acquisitions, and significant changes or reassignments of personnel with responsibility for security controls.

Definitions

Examples

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.6

12.6 Security awareness education is an ongoing activity.

DEFINED APPROACH REQUIREMENTS

12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity’s information security policy and procedures, and their role in protecting the cardholder data.

CUSTOMIZED APPROACH OBJECTIVE

Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.6.1 Examine the security awareness program to verify it provides awareness to all personnel about the entity's information security policy and procedures, and personnel's role in protecting the cardholder data.

GUIDANCE

Purpose

If personnel are not educated about their company's information security policies and procedures and their own security responsibilities, security safeguards and processes that have been implemented may become ineffective through unintentional errors or intentional actions.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.6.2 The security awareness program is:

- Reviewed at least once every 12 months, and
- Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.

CUSTOMIZED APPROACH OBJECTIVE

The content of security awareness material is reviewed and updated periodically.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.6.2 Examine security awareness program content, evidence of reviews, and interview personnel to verify that the security awareness program is in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

The threat environment and an entity's defenses are not static. As such, the security awareness program materials must be updated as frequently as needed to ensure that the education received by personnel is up to date and represents the current threat environment.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.6.3 Personnel receive security awareness training as follows:

- Upon hire and at least once every 12 months.
- Multiple methods of communication are used.
- Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.

CUSTOMIZED APPROACH OBJECTIVE

Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.6.3.a Examine security awareness program records to verify that personnel attend security awareness training upon hire and at least once every 12 months.

12.6.3.b Examine security awareness program materials to verify the program includes multiple methods of communicating awareness and educating personnel.

12.6.3.c Interview personnel to verify they have completed awareness training and are aware of their role in protecting cardholder data.

12.6.3.d Examine security awareness program materials and personnel acknowledgments to verify that personnel acknowledge at least once every 12 months that they have read and understand the information security policy and procedures.

GUIDANCE

Purpose

Training of personnel ensures they receive the information about the importance of information security and that they understand their role in protecting the organization. Requiring an acknowledgment by personnel helps ensure that they have read and understood the security policies and procedures, and that they have made and will continue to make a commitment to comply with these policies.

Good Practice

Entities may incorporate new-hire training as part of the Human Resources onboarding process. Training should outline the security-related “dos” and “don’ts.” Periodic refresher training reinforces key security processes and procedures that may be forgotten or bypassed.

Entities should consider requiring security awareness training anytime personnel transfer into roles where they can impact the security of account data from roles where they did not have this impact.

Methods and training content can vary, depending on personnel roles.

Definitions

Examples

Different methods that can be used to provide security awareness and education include posters, letters, web-based training, in-person training, team meetings, and incentives.

Personnel acknowledgments may be recorded in writing or electronically.

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:

- Phishing and related attacks.
- Social engineering.

CUSTOMIZED APPROACH OBJECTIVE

Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.

APPLICABILITY NOTES

See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.6.3.1 Examine security awareness training content to verify it includes all elements specified in this requirement.

GUIDANCE

Purpose

Educating personnel on how to detect, react to, and report potential phishing and related attacks and social engineering attempts is essential to minimizing the probability of successful attacks.

Good Practice

An effective security awareness program should include examples of phishing emails and periodic testing to determine the prevalence of personnel reporting such attacks. Training material an entity can consider for this topic include:

- How to identify phishing and other social engineering attacks.
- How to react to suspected phishing and social engineering.
- Where and how to report suspected phishing and social engineering activity. An emphasis on reporting allows the organization to reward positive behavior, to optimize technical defenses (see Requirement 5.4.1), and to take immediate action to remove similar phishing emails that evaded technical defenses from recipient inboxes.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.

CUSTOMIZED APPROACH OBJECTIVE

Personnel are knowledgeable about their responsibility for the security and operation of end-user technologies and are able to access assistance and guidance when required.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.6.3.2 Examine security awareness training content to verify it includes awareness about acceptable use of end-user technologies in accordance with Requirement 12.2.1.

GUIDANCE

Purpose

By including the key points of the acceptable use policy in regular training and the related context, personnel will understand their responsibilities and how these impact the security of an organization's systems.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.7

12.7 Personnel are screened to reduce risks from insider threats.

DEFINED APPROACH REQUIREMENTS

12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.

CUSTOMIZED APPROACH OBJECTIVE

The risk related to allowing new members of staff access to the CDE is understood and managed.

APPLICABILITY NOTES

For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.

DEFINED APPROACH TESTING PROCEDURES

12.7.1 Interview responsible Human Resource department management to verify that screening is conducted, within the constraints of local laws, prior to hiring potential personnel who will have access to the CDE.

GUIDANCE

Purpose

Performing thorough screening prior to hiring potential personnel who are expected to be given access to the CDE provides entities with the information necessary to make informed risk decisions regarding personnel they hire that will have access to the CDE.

Other benefits of screening potential personnel include helping to ensure workplace safety and confirming information provided by prospective employees on their resumes.

Good Practice

Entities should consider screening for existing personnel anytime they transfer into roles where they have access to the CDE from roles where they did not have this access.

To be effective, the level of screening should be appropriate for the position. For example, positions requiring greater responsibility or that have administrative access to critical data or systems may warrant more detailed or more frequent screening than positions with less responsibility and access.

Definitions

Examples

Screening options can include, as appropriate for the entity's region, previous employment history, review of public information/social media resources, criminal record, credit history, and reference checks.

Further Information

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.8

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

DEFINED APPROACH REQUIREMENTS

12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

CUSTOMIZED APPROACH OBJECTIVE

Records are maintained of TPSPs and the services provided.

APPLICABILITY NOTES

The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.

DEFINED APPROACH TESTING PROCEDURES

12.8.1.a Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.

12.8.1.b Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.

GUIDANCE

Purpose

Maintaining a list of all TPSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface.

Good Practice

Definitions

Examples

Different types of TPSPs include those that:

- Store, process, or transmit account data on the entity's behalf (such as payment gateways, payment processors, payment service providers (PSPs), and off-site storage providers).
- Manage system components included in the entity's PCI DSS assessment (such as providers of network security control services, anti-malware services, and security incident and event management (SIEM); contact and call centers; web-hosting companies; and IaaS, PaaS, SaaS, and FaaS cloud providers).
- Could impact the security of the entity's CDE (such as vendors providing support via remote access, and bespoke software developers).

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.8.2 Written agreements with TPSPs are maintained as follows:

- Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
- Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.

CUSTOMIZED APPROACH OBJECTIVE

Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.

APPLICABILITY NOTES

The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.

Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.

DEFINED APPROACH TESTING PROCEDURES

12.8.2.a Examine policies and procedures to verify that processes are defined to maintain written agreements with all TPSPs in accordance with all elements specified in this requirement.

12.8.2.b Examine written agreements with TPSPs to verify they are maintained in accordance with all elements as specified in this requirement.

GUIDANCE

Purpose

The written acknowledgment from a TPSP demonstrates its commitment to maintaining proper security of account data that it obtains from its customers and that the TPSP is fully

aware of the assets that could be affected during the provisioning of the TPSP's service. The extent to which a specific TPSP is responsible for the security of account data will depend on the service provided and the agreement between the provider and assessed entity (the customer).

In conjunction with Requirement 12.9.1, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.

Good Practice

The entity may also want to consider including in their written agreement with a TPSP that the TPSP will support the entity's request for information per Requirement 12.9.2. Entities will also want to understand whether any TPSPs have "nested" relationships with other TPSPs, meaning the primary TPSP contracts with another TPSP(s) for the purposes of providing a service.

It is important to understand whether the primary TPSP is relying on the secondary TPSP(s) to achieve overall compliance of a service, and what types of written agreements the primary TPSP has in place with the secondary TPSPs. Entities can consider including coverage in their written agreement for any "nested" TPSPs a primary TPSP may use.

Definitions

Examples

Further Information

Refer to the *"Information Supplement: Third-Party Security Assurance* for further guidance.

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

CUSTOMIZED APPROACH OBJECTIVE

The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.8.3.a Examine policies and procedures to verify that processes are defined for engaging TPSPs, including proper due diligence prior to engagement.

12.8.3.b Examine evidence and interview responsible personnel to verify the process for engaging TPSPs includes proper due diligence prior to engagement.

GUIDANCE

Purpose

A thorough process for engaging TPSPs, including details for selection and vetting prior to engagement, helps ensure that a TPSP is thoroughly vetted internally by an entity prior to establishing a formal relationship and that the risk to cardholder data associated with the engagement of the TPSP is understood.

Good Practice

Specific due-diligence processes and goals will vary for each organization. Elements that should be considered include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the TPSP validates their PCI DSS compliance and what evidence they provide.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.

CUSTOMIZED APPROACH OBJECTIVE

The PCI DSS compliance status of TPSPs is verified periodically.

APPLICABILITY NOTES

Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those r

DEFINED APPROACH TESTING PROCEDURES

12.8.4.a Examine policies and procedures to verify that processes are defined to monitor TPSPs' PCI DSS compliance status at least once every 12 months.

12.8.4.b Examine documentation and interview responsible personnel to verify that the PCI DSS compliance status of each TPSP is monitored at least once every 12 months.

GUIDANCE

Purpose

Knowing the PCI DSS compliance status of all engaged TPSPs provides assurance and awareness about whether they comply with the requirements applicable to the services they offer to the organization.

Good Practice

If the TPSP offers a variety of services, the compliance status the entity monitors should be specific to those services delivered to the entity and those services in scope for the entity's PCI DSS assessment.

If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status.

If the TPSP did not undergo a PCI DSS assessment, it may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met.

Definitions

Examples

Further Information

For more information about third-party service providers, refer to:

- PCI DSS section: *Use of Third-Party Service Providers*.
- *Information Supplement: Third-Party Security Assurance*.

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.

CUSTOMIZED APPROACH OBJECTIVE

Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.8.5.a Examine policies and procedures to verify that processes are defined to maintain information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both the TPSP and the entity.

12.8.5.b Examine documentation and interview personnel to verify the entity maintains information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both entities.

GUIDANCE

Purpose

It is important that the entity understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the entity, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement.

Without this shared understanding, it is inevitable that the entity and the TPSP will assume a given PCI DSS sub-requirement is the responsibility of the other party, and therefore that

sub-requirement may not be addressed at all.

The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the entity and TPSP.

Good Practice

Entities can document these responsibilities via a matrix that identifies all applicable PCI DSS requirements and indicates for each requirement whether the entity or TPSP is responsible for meeting that requirement or whether it is a shared responsibility. This type of document is often referred to as a *responsibility matrix*.

It is also important for entities to understand whether any TPSPs have "nested" relationships with other TPSPs, meaning the primary TPSP contracts with another TPSP(s) for the purposes of providing a service. It is important to understand whether the primary TPSP is relying on the secondary TPSP(s) to achieve overall compliance of a service, and how the primary TPSP is monitoring performance of the service and the PCI DSS compliance status of the secondary TPSP(s). Note that it is the responsibility of the primary TPSP to manage and monitor any secondary TPSPs.

Definitions

Examples

Further Information

Refer to *Information Supplement: Third-Party Security Assurance* for a sample responsibility matrix template.

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.9

12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

DEFINED APPROACH REQUIREMENTS

12.9.1 Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.

CUSTOMIZED APPROACH OBJECTIVE

TPSPs formally acknowledge their security responsibilities to their customers.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.

DEFINED APPROACH TESTING PROCEDURES

12.9.1 Additional testing procedure for service provider assessments only: Examine TPSP policies, procedures, and templates used for written agreements to verify processes are defined for the TPSP to provide written acknowledgments to customers in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between TPSPs and their customers about their applicable PCI DSS responsibilities. The acknowledgment of the TPSPs evidences their commitment to maintaining proper security of account data that it obtains from its clients.

The method by which the TPSP provides written acknowledgment should be agreed between the provider and its customers.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request:

- PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4).
- Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).

CUSTOMIZED APPROACH OBJECTIVE

TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

12.9.2 Additional testing procedure for service provider assessments only: Examine policies and procedures to verify processes are defined for the TPSPs to support customers' request for information to meet Requirements 12.8.4 and 12.8.5 in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

If a TPSP does not provide the necessary information to enable its customers to meet their security and compliance requirements, the customers will not be able to protect cardholder data nor meet their own contractual obligations.

Good Practice

If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status.

If the TPSP did not undergo a PCI DSS assessment, they may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific

evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met.

TPSPs should provide sufficient evidence to their customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place.

TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the customer and TPSP. It is important that the customer understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the customer, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement. An example of a way to document these responsibilities is via a matrix that identifies all applicable PCI DSS requirements and indicates whether the customer or TPSP is responsible for meeting that requirement or whether it is a shared responsibility.

Definitions

Examples

Further Information

For further guidance, refer to:

- PCI DSS section: *Use of Third-Party Service Providers*.
- *Information Supplement: Third-Party Security Assurance* (includes a sample responsibility matrix template).

sections 12 | top

REQUIREMENTS and TESTING PROCEDURES 12.10

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

DEFINED APPROACH REQUIREMENTS

12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:

- Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
- Incident response procedures with specific containment and mitigation activities for different types of incidents.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

CUSTOMIZED APPROACH OBJECTIVE

A comprehensive incident response plan that meets card brand expectations is maintained.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.10.1.a Examine the incident response plan to verify that the plan exists and includes at least the elements specified in this requirement.

12.10.1.b Interview personnel and examine documentation from previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.

GUIDANCE

Purpose

Without a comprehensive incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as risk of financial and/or reputational loss and legal liabilities.

Good Practice

The incident response plan should be thorough and contain all the key elements for stakeholders (for example, legal, communications) to allow the entity to respond effectively in the event of a breach that could impact account data. It is important to keep the plan up to date with current contact information of all individuals designated as having a role in

incident response. Other relevant parties for notifications may include customers, financial institutions (acquirers and issuers), and business partners.

Entities should consider how to address all compromises of data within the CDE in their incident response plans, including to account data, wireless encryption keys, encryption keys used for transmission and storage or account data or cardholder data, etc.

Definitions

Examples

Legal requirements for reporting compromises include those in most US states, the EU General Data Protection Regulation (GDPR), and the Personal Data Protection Act (Singapore).

Further Information

For more information, refer to the *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.2 At least once every 12 months, the security incident response plan is:

- Reviewed and the content is updated as needed.
- Tested, including all elements listed in Requirement 12.10.1.

CUSTOMIZED APPROACH OBJECTIVE

The incident response plan is kept current and tested periodically.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.10.2 Interview personnel and review documentation to verify that, at least once every 12 months, the security incident response plan is:

- Reviewed and updated as needed.
- Tested, including all elements listed in Requirement 12.10.1.

GUIDANCE

Purpose

Proper testing of the security incident response plan can identify broken business processes and ensure key steps are not missed, which could result in increased exposure during an incident. Periodic testing of the plan ensures that the processes remain viable, as well as ensuring that all relevant personnel in the organization are familiar with the plan.

Good Practice

The test of the incident response plan can include simulated incidents and the corresponding responses in the form of a “table-top exercise”, that include participation by relevant personnel. A review of the incident and the quality of the response can provide entities with the assurance that all required elements are included in the plan.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.

CUSTOMIZED APPROACH OBJECTIVE

Incidents are responded to immediately where appropriate.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.10.3 Examine documentation and interview responsible personnel occupying designated roles to verify that specific personnel are designated to be available on a 24/7 basis to respond to security incidents.

GUIDANCE

Purpose

An incident could occur at any time, therefore if a person who is trained in incident response and familiar with the entity's plan is available when an incident is detected, the entity's ability to correctly respond to the incident is increased.

Good Practice

Often, specific personnel are designated to be part of a security incident response team, with the team having overall responsibility for responding to incidents (perhaps on a rotating schedule basis) and managing those incidents in accordance with the plan. The incident response team can consist of core members who are permanently assigned or "on-demand" personnel who may be called up as necessary, depending on their expertise and the specifics of the incident.

Having available resources to respond quickly to incidents minimizes disruption to the organization.

Examples of types of activity the team or individuals should respond to include any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.

CUSTOMIZED APPROACH OBJECTIVE

Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.10.4 Examine training documentation and interview incident response personnel to verify that personnel are appropriately and periodically trained on their incident response responsibilities.

GUIDANCE

Purpose

Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become “polluted” by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.

Good Practice

It is important that all personnel involved in incident response are trained and knowledgeable about managing evidence for forensics and investigations.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

CUSTOMIZED APPROACH OBJECTIVE

Incident response personnel are trained at a frequency that addresses the entity’s risk.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.10.4.1.a Examine the entity's targeted risk analysis for the frequency of training for incident response personnel to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.

12.10.4.1.b Examine documented results of periodic training of incident response personnel and interview personnel to verify training is performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.

GUIDANCE

Purpose

Each entity's environment and incident response plan are different and the approach will depend on a number of factors, including the size and complexity of the entity, the degree of change in the environment, the size of the incident response team, and the turnover in personnel. Performing a risk analysis will allow the entity to determine the optimum frequency for training personnel with incident response responsibilities.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:

- Intrusion-detection and intrusion-prevention systems.
- Network security controls.
- Change-detection mechanisms for critical files.
- The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details*.
- Detection of unauthorized wireless access points.

CUSTOMIZED APPROACH OBJECTIVE

Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.

APPLICABILITY NOTES

The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.10.5 Examine documentation and observe incident response processes to verify that monitoring and responding to alerts from security monitoring systems are covered in the security incident response plan, including but not limited to the systems specified in this requirement.

GUIDANCE

Purpose

Responding to alerts generated by security monitoring systems that are explicitly designed to focus on potential risk to data is critical to prevent a breach and therefore, this must be included in the incident-response processes.

Good Practice

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.

CUSTOMIZED APPROACH OBJECTIVE

The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

12.10.6.a Examine policies and procedures to verify that processes are defined to modify and evolve the security incident response plan according to lessons learned and to incorporate industry developments.

12.10.6.b Examine the security incident response plan and interview responsible personnel to verify that the incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.

GUIDANCE

Purpose

Incorporating lessons learned into the incident response plan after an incident occurs and in-step with industry developments, helps keep the plan current and able to react to emerging threats and security trends.

Good Practice

The lessons-learned exercise should include all levels of personnel. Although it is often included as part of the review of the entire incident, it should focus on how the entity's response to the incident could be improved.

It is important to not just consider elements of the response that did not have the planned outcomes but also to understand what worked well and whether lessons from those elements that worked well can be applied areas of the plan that didn't.

Another way to optimize an entity's incident response plan is to understand the attacks made against other organizations and use that information to fine-tune the entity's detection, containment, mitigation, or recovery procedures.

Definitions

Examples

Further Information

sections 12 | top

DEFINED APPROACH REQUIREMENTS

12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include:

- Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.
- Identifying whether sensitive authentication data is stored with PAN.
- Determining where the account data came from and how it ended up where it was not expected.
- Remediating data leaks or process gaps that resulted in the account data being where it was not expected.

CUSTOMIZED APPROACH OBJECTIVE

Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

12.10.7.a Examine documented incident response procedures to verify that procedures for responding to the detection of stored PAN anywhere it is not expected to exist, ready to be initiated, and include all elements specified in this requirement.

12.10.7.b Interview personnel and examine records of response actions to verify that incident response procedures are performed upon detection of stored PAN anywhere it is not expected.

GUIDANCE

Purpose

Having documented incident response procedures that are followed in the event that stored PAN is found anywhere it is not expected to be, helps to identify the necessary remediation actions and prevent future leaks.

Good Practice

If PAN was found outside the CDE, analysis should be performed to 1) determine whether it was saved independently of other data or with sensitive authentication data, 2) identify the source of the data, and 3) identify the control gaps that resulted in the data being outside the CDE.

Entities should consider whether there are contributory factors, such as business processes, user behavior, improper system configurations, etc. that caused the PAN to be stored in an unexpected location. If such contributory factors are present, they should be addressed per this Requirement to prevent recurrence.

Definitions

Examples

Further Information

sections 12 | top

Appendix A Additonal PCI Requirements

OVERVIEW

This appendix contains additional PCI DSS requirements for different types of entities.

Guidance and applicability information is provided in each section.

SECTIONS A

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/early TLS for Card-Present POS POI Terminal Connections

Appendix A3: Designated Entities Supplemental Validation (DESV)

Appendix A | appendices | principles | top

Appendix A Additonal PCI Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

OVERVIEW

All service providers are responsible for meeting PCI DSS requirements for their own environments as applicable to the services offered to their customers. In addition, multi-tenant service providers must meet the requirements in this Appendix.

Multi-tenant service providers are a type of third-party service provider that offers various shared services to merchants and other service providers, where customers share system resources (such as physical or virtual servers), infrastructure, applications (including Software as a Service (SaaS)), and/or databases. Services may include, but are not limited to, hosting multiple entities on a single shared server, providing e-commerce and/or "shopping cart" services, web- based hosting services, payment applications, various cloud applications and services, and connections to payment gateways and processors.

Service providers that provide only shared data center services (often called co-location or "co-lo" providers), where equipment, space, and bandwidth are available on a rental basis, are not considered multi-tenant service providers for purposes of this Appendix.

Note: Even though a multi-tenant service provider may meet these requirements, each customer is still responsible to comply with the PCI DSS requirements that are applicable to its environment and validate compliance as applicable. Often, there are PCI DSS requirements for which responsibility is shared between the provider and the customer (for perhaps different aspects of the environment). Requirements 12.8 and 12.9 delineate requirements specific to the relationships between all third-party service providers (TPSPs) and their customers, and the responsibilities of both. This includes defining the specific services the customer is receiving, along with which PCI DSS requirements are the responsibility of the customer to meet, which are the responsibility of the TPSP, and which requirements are shared between both customer and the TPSP.

SECTIONS A1

A1.1 Multi-tenant service providers protect and separate all customer environments and data.

A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.

Appendix A1 | appendices | principles | top

REQUIREMENTS and TESTING PROCEDURES A1.1

A1.1 Multi-tenant service providers protect and separate all customer environments and data.

DEFINED APPROACH REQUIREMENTS

A1.1.1 Logical separation is implemented as follows:

- The provider cannot access its customers' environments without authorization.
- Customers cannot access the provider's environment without authorization.

CUSTOMIZED APPROACH OBJECTIVE

Customers cannot access the provider's environment. The provider cannot access its customers' environments without authorization.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

A1.1.1 Examine documentation and system and network configurations and interview personnel to verify that logical separation is implemented in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Without controls between the provider's environment and the customer's environment, a malicious actor within the provider's environment could compromise the customer's environment, and similarly, a malicious actor in a customer environment could compromise the provider and potentially other of the provider's customers.

Multi-tenant environments should be isolated from each other and from the provider's infrastructure such that they can be separately managed entities with no connectivity between them.

Good Practice

Providers should ensure strong separation between the environments that are designed for customer access, for example, configuration and billing portals, and the provider's private environment that should only be accessed by authorized provider personnel. Service provider access to customer environments is performed in accordance with requirement 8.2.3.

Definitions

Examples

Further Information

Refer to the *Information Supplement: PCI SSC Cloud Computing Guidelines* for further guidance on cloud environments.

Section A1 | top

DEFINED APPROACH REQUIREMENTS

A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.

CUSTOMIZED APPROACH OBJECTIVE

Customers cannot access other customers' environments.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

A1.1.2.a Examine documentation to verify controls are defined such that each customer only has permission to access its own cardholder data and CDE.

A1.1.2.b Examine system configurations to verify that customers have privileges established to only access their own account data and CDE.

GUIDANCE

Purpose

It is important that a multi-tenant service provider define controls so that each customer can only access their own environment and CDE to prevent unauthorized access from one customer's environment to another.

Good Practice

Definitions

Examples

In a cloud-based infrastructure, such as an infrastructure as a service (IaaS) offering, the customers' CDE may include virtual network devices and virtual servers that are configured and managed by the customers, including operating systems, files, memory, etc.

Further Information

Section A1 | top

DEFINED APPROACH REQUIREMENTS

A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.

CUSTOMIZED APPROACH OBJECTIVE

Customers cannot impact resources allocated to other customers.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

A1.1.3 Examine customer privileges to verify each customer can only access resources allocated to them.

GUIDANCE

Purpose

To prevent any inadvertent or intentional impact to other customers' environments or account data, it is important that each customer can access only resources allocated to that customer

Good Practice

Definitions

Examples

Further Information

Section A1 | top

DEFINED APPROACH REQUIREMENTS

A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.

CUSTOMIZED APPROACH OBJECTIVE

Segmentation of customer environments from other environments is periodically validated to be effective.

APPLICABILITY NOTES

The testing of adequate separation between customers in a multi-tenant service provider environment is in addition to the penetration tests specified in Requirement 11.4.6. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

A1.1.4 Examine the results from the most recent penetration test to verify that testing confirmed the effectiveness of logical separation controls used to separate customer environments.

GUIDANCE

Purpose

Multi-tenant services providers are responsible for managing the segmentation between their customers.

Without technical assurance that segmentation controls are effective, it is possible that changes to the service provider's technology would inadvertently create a vulnerability that could be exploited across all the service provider's customers.

Good Practice

Effectiveness of separation techniques can be confirmed by using service-provider-created temporary (mock-up) environments that represent customer environments and attempting

to 1) access one temporary environment from another environment, and 2) access a temporary environment from the Internet.

Definitions

Examples

Further Information

Section A1 | top

REQUIREMENTS and TESTING PROCEDURES A1.2

A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.

DEFINED APPROACH REQUIREMENTS

A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including:

- Logs are enabled for common third-party applications.
- Logs are active by default.
- Logs are available for review only by the owning customer.
- Log locations are clearly communicated to the owning customer.
- Log data and availability is consistent with PCI DSS Requirement 10.

CUSTOMIZED APPROACH OBJECTIVE

Log capability is available to all customers without affecting the confidentiality of other customers.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

A1.2.1 Examine documentation and system configuration settings to verify the provider has enabled audit log capability for each customer environment in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Log information is useful for detecting and troubleshooting security incidents and is invaluable for forensic investigations. Customers therefore need to have access to these logs.

However, log information can also be used by an attacker for reconnaissance, and so a customer's log information must only be accessible by the customer that the log relates to.

Good Practice

Definitions

Examples

Further Information

Section A1 | top

DEFINED APPROACH REQUIREMENTS

A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.

CUSTOMIZED APPROACH OBJECTIVE

Forensic investigation is readily available to all customers in the event of a suspected or confirmed security incident.

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

A1.2.2 Examine documented procedures to verify that the provider has processes or mechanisms to support and/or facilitate a prompt forensic investigation of related servers in the event of a suspected or confirmed security incident for any customer.

GUIDANCE

Purpose

In the event of a suspected or confirmed breach of confidentiality of cardholder data, a customer's forensic investigator aims to find the cause of the breach, exclude the attacker from the environment, and ensure all unauthorized access is removed. Prompt and efficient

responses to forensic investigators' requests can significantly reduce the time taken for the investigator to secure the customer's environment.

Good Practice

Definitions

Examples

Further Information

Section A1 | top

DEFINED APPROACH REQUIREMENTS

A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including:

- Customers can securely report security incidents and vulnerabilities to the provider.
- The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.

CUSTOMIZED APPROACH OBJECTIVE

Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.

APPLICABILITY NOTES

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

DEFINED APPROACH TESTING PROCEDURES

A1.2.3 Examine documented procedures and interview personnel to verify that the provider has a mechanism for reporting and addressing suspected or confirmed security incidents and vulnerabilities, in accordance with all elements specified in this requirement.

GUIDANCE

Purpose

Security vulnerabilities in the provided services can impact the security of all the service provider's customers and therefore must be managed in accordance with the service provider's established processes, with priority given to resolving vulnerabilities that have the highest probability of compromise.

Customers are likely to notice vulnerabilities and security misconfigurations while using the service.

Implementing secure methods for customers to report security incidents and vulnerabilities encourages customers to report potential issues and enable the provider to quickly learn about and address potential issues within their environment.

Good Practice

Definitions

Examples

Further Information

Section A1 | top

Appendix A Additonal PCI Requirements

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections

OVERVIEW

This Appendix applies only to entities using SSL/early TLS as a security control to protect POS POI terminals, including service providers that provide connections into POS POI terminals.

Entities using SSL and early TLS for POS POI terminal connections must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment terminals. However, new vulnerabilities could emerge at any time, and it is up to

the organization to remain up to date with vulnerability trends and determine whether it is susceptible to any known exploits.

The PCI DSS requirements directly affected are: • Requirement 2.2.5: Where any insecure services, protocols, or daemons are present; business justification is documented, and additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. • Requirement 2.2.7: All non-console administrative access is encrypted using strong cryptography. • Requirement 4.2.1: Strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks. SSL and early TLS must not be used as a security control to meet these requirements, except in the case of POS POI terminal connections, as detailed in this appendix. To support entities working to migrate from SSL/early TLS on POS POI terminals, the following provisions are included: • New POS POI terminal implementations must not use SSL or early TLS as a security control. • All POS POI terminal service providers must provide a secure service offering. • Service providers supporting existing POS POI terminal implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. • POS POI terminals in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, and the SSL/TLS termination points to which they connect, may continue using SSL/early TLS as a security control.

Requirements in this Appendix are not eligible for the Customized Approach.

SECTIONS A2

A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.

Appendix A2 | appendices | principles | top

REQUIREMENTS and TESTING PROCEDURES A2.1

A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.

DEFINED APPROACH REQUIREMENTS

A2.1.1 Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.1.2 and A2.1.3 apply to POS POI service providers.

The allowance for POS POI terminals that are not currently susceptible to exploits is based on currently known risks. If new exploits are introduced to which POS POI terminals are susceptible, the POS POI terminals will need to be updated immediately.

DEFINED APPROACH TESTING PROCEDURES

A2.1.1 For POS POI terminals using SSL and/or early TLS, confirm the entity has documentation (for example, vendor documentation, system/network configuration details) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.

GUIDANCE

Purpose

POS POI terminals used in card-present environments can continue using SSL/early TLS when it can be shown that the POS POI terminal is not susceptible to the currently known exploits.

Good Practice

However, SSL is outdated technology and could be susceptible to additional security vulnerabilities in the future; it is therefore strongly recommended that POS POI terminals be upgraded to a secure protocol as soon as possible. If SSL/early TLS is not needed in the environment, use of, and fallback to these versions should be disabled.

Definitions

Examples

Further Information

Refer to the current PCI SSC Information Supplements on SSL/Early TLS for further guidance.

Section A2 | top

DEFINED APPROACH REQUIREMENTS

A2.1.2 Additional requirement for service providers only: All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes:

- Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment.
- Risk-assessment results and risk-reduction controls in place.
- Description of processes to monitor for new vulnerabilities associated with SSL/early TLS.
- Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments.
- Overview of migration project plan to replace SSL/early TLS at a future date.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

A2.1.2 Additional testing procedure for service provider assessments only: Review the documented Risk Mitigation and Migration Plan to verify it includes all elements specified in this requirement.

GUIDANCE

Purpose

POS POI termination points, including but not limited to service providers such as acquirers or acquirer processors, can continue using SSL/early TLS when it can be shown that the service provider has controls in place that mitigate the risk of supporting those connections for the service provider environment.

Good Practice

Service providers should communicate to all customers using SSL/early TLS about the risks associated with its use and the need to migrate to a secure protocol.

Definitions

The Risk Mitigation and Migration Plan is a document prepared by the entity that details its plans for migrating to a secure protocol and describes controls the entity has in place to reduce the risk associated with SSL/early TLS until the migration is complete.

Examples

Further Information

Refer to the current PCI SSC Information Supplements on SSL/early TLS for further guidance on Risk Mitigation and Migration Plans.

Section A2 | top

DEFINED APPROACH REQUIREMENTS

A2.1.3 Additional requirement for service providers only: All service providers provide a secure service offering.

CUSTOMIZED APPROACH OBJECTIVE

This requirement is not eligible for the customized approach.

APPLICABILITY NOTES

This requirement applies only when the entity being assessed is a service provider.

DEFINED APPROACH TESTING PROCEDURES

A2.1.3 Additional testing procedure for service provider assessments only: Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for its service.

GUIDANCE

Purpose

Customers must be able to choose to upgrade their POIs to eliminate the vulnerability in using SSL and early TLS. In many cases, customers will need to take a phased or gradual approach to migrate their POS POI estate from the insecure protocol to a secure protocol and so will require the service provider to support a secure offering.

Good Practice

Refer to the current PCI SSC Information Supplements on SSL/Early TLS for further guidance.

Definitions

Examples

Further Information

Section A2 | top

Appendix A Additonal PCI Requirements

Appendix A3: Designated Entities Supplemental Validation (DESV)

OVERVIEW

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. An entity is required to undergo an assessment according to this Appendix ONLY if instructed to do so by an acquirer or a payment brand. Examples of entities that this Appendix could apply to include:

- Those storing, processing, and/or transmitting large volumes of account data,
- Those providing aggregation points for account data, or
- Those that have suffered significant or repeated breaches of account data. Additionally, other PCI standards may reference completion of this Appendix.

These supplemental validation steps are intended to provide greater assurance that PCI DSS controls are maintained effectively and on a continuous basis through validation of business-as-usual (BAU) processes and increased validation and scoping consideration.

Note: Some requirements have defined timeframes (for example, at least once every three months or at least once every six months) within which certain activities are to be performed. For initial assessment to this document, it is not required that an activity has been performed for every such timeframe during the previous year, if the assessor verifies:

- The activity was performed in accordance with the applicable requirement within the most recent timeframe (for example, the most recent three-month or six-month period), and
- The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe. For subsequent years after the initial assessment, an activity must have been performed within each required timeframe (for example, an activity required every three months must have been performed at least four times during the previous year at an interval that does not exceed 90 days).

Not all requirements in PCI DSS apply to all entities that may undergo a PCI DSS assessment. It is for this reason that some PCI DSS Requirements are duplicated in this appendix. Any questions about this appendix should be addressed to acquirers or payment brands.

SECTIONS A3

A3.1 A PCI DSS compliance program is implemented.

A3.2 PCI DSS scope is documented and validated.

A3.3 PCI DSS is incorporated into business-as-usual (BAU) activities.

A3.4 Logical access to the cardholder data environment is controlled and managed.

A3.5 Suspicious events are identified and responded to.

Appendix A3 | appendices | principles | top

REQUIREMENTS and TESTING PROCEDURES A3.1

A3.1 A PCI DSS compliance program is implemented.

DEFINED APPROACH REQUIREMENTS

A3.1.1 Responsibility is established by executive management for the protection of account data and a PCI DSS compliance program that includes:

- Overall accountability for maintaining PCI DSS compliance.
- Defining a charter for a PCI DSS compliance program.
- Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least once every 12 months.

PCI DSS Reference: Requirement 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.1.2 A formal PCI DSS compliance program is in place that includes:

- Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities.
- Annual PCI DSS assessment processes.
- Processes for the continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement).
- A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions.

PCI DSS Reference: Requirements 1-12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.1.3 PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel, including:

- Managing PCI DSS business-as-usual activities.
- Managing annual PCI DSS assessments.
- Managing continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement).
- Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. PCI DSS Reference: Requirement 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.1.4 Up-to-date PCI DSS and/or information security training is provided at least once every 12 months to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). PCI DSS Reference: Requirement 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

REQUIREMENTS and TESTING PROCEDURES A3.2

A3.2 PCI DSS scope is documented and validated.

DEFINED APPROACH REQUIREMENTS

A3.2.1 PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in-scope environment. At a minimum, the scoping validation includes:

- Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).
- Updating all data-flow diagrams per Requirement 1.2.4.
- Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2)

applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.
- For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it.
- Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.
- Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.
- Identifying all connections to third-party entities with access to the CDE.
- Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12.

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.2 PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include:

- Performing a formal PCI DSS impact assessment.
- Identifying applicable PCI DSS requirements to the system or network.
- Updating PCI DSS scope as appropriate.

- Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). PCI DSS Reference: Scope of PCI DSS Requirements; Requirements 1-12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.2.1 Upon completion of a change, all relevant PCI DSS requirements are confirmed to be implemented on all new or changed systems and networks, and documentation is updated as applicable. PCI DSS Reference: Scope of PCI DSS Requirements; Requirement 1-12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.3 Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. PCI DSS Reference: Requirement 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.4 If segmentation is used, PCI DSS scope is confirmed as follows:

- Per the entity's methodology defined at Requirement 11.4.1.
- Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods.
- The penetration testing covers all segmentation controls/methods in use.
- The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. PCI DSS Reference: Requirement 11

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.5 A data-discovery methodology is implemented that:

- Confirms PCI DSS scope.
- Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes.
- Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.5.1 Data discovery methods are confirmed as follows:

- Effectiveness of methods is tested.
- Methods are able to discover cleartext PAN on all types of system components and file formats in use.
- The effectiveness of data-discovery methods is confirmed at least once every 12 months. PCI DSS Reference: Scope of PCI DSS Requirements

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.5.2 Response procedures are implemented to be initiated upon the detection of cleartext PAN outside the CDE to include:

- Determining what to do if cleartext PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.
- Determining how the data ended up outside the CDE.

- Remediating data leaks or process gaps that resulted in the data being outside the CDE.
- Identifying the source of the data.
- Identifying whether any track data is stored with the PANs.

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.6 Mechanisms are implemented for detecting and preventing cleartext PAN from leaving the CDE via an unauthorized channel, method, or process, including mechanisms that are:

- Actively running.
- Configured to detect and prevent cleartext PAN leaving the CDE via an unauthorized channel, method, or process.
- Generating audit logs and alerts upon detection of cleartext PAN leaving the CDE via an unauthorized channel, method, or process. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include:

- Procedures for the prompt investigation of alerts by responsible personnel.
- Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

REQUIREMENTS and TESTING PROCEDURES A3.3

A3.3 PCI DSS is incorporated into business-as-usual (BAU) activities.

DEFINED APPROACH REQUIREMENTS

A3.3.1 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of:

- Network security controls
- IDS/IPS
- FIM
- Anti-malware solutions
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)
- Automated audit log review mechanisms. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
- Automated code review tools (if used). This bullet is a best practice until its effective date; refer to Applicability Notes below for details. PCI DSS Reference: Requirements 1-12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.3.1.2 Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include:

- Restoring security functions.
- Identifying and documenting the duration (date and time from start to end) of the security failure.
- Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause.
- Identifying and addressing any security issues that arose during the failure.
- Determining whether further actions are required as a result of the security failure.
- Implementing controls to prevent the cause of failure from reoccurring.
- Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.3.2 Hardware and software technologies are reviewed at least once every 12 months to confirm whether they continue to meet the organization’s PCI DSS requirements. PCI DSS Reference: Requirements 2, 6, 12.

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

DEFINED APPROACH REQUIREMENTS

A3.3.3 Reviews are performed at least once every three months to verify BAU activities are being followed. Reviews are performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include:

- Confirmation that all BAU activities, including A3.2.2, A3.2.6, and A3.3.1, are being performed.
- Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, ruleset reviews for network security controls, configuration standards for new systems).
- Documenting how the reviews were completed, including how all BAU activities were verified as being in place.
- Collection of documented evidence as required for the annual PCI DSS assessment.
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program, as identified in A3.1.3.
- Retention of records and documentation for at least 12 months, covering all BAU activities. PCI DSS Reference: Requirements 1-12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

REQUIREMENTS and TESTING PROCEDURES A3.4

A3.4 Logical access to the cardholder data environment is controlled and managed.

DEFINED APPROACH REQUIREMENTS

A3.4.1 User accounts and access privileges to in-scope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized. PCI DSS Reference: Requirement 7

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

REQUIREMENTS and TESTING PROCEDURES A3.5

A3.5 Suspicious events are identified and responded to.

DEFINED APPROACH REQUIREMENTS

A3.5.1 A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes:

- Identification of anomalies or suspicious activity as it occurs.
- Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel.
- Response to alerts in accordance with documented response procedures. PCI DSS Reference: Requirements 10, 12

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

Appendix B Compensating Controls

OVERVIEW

Compensating controls may be considered when an entity cannot meet a PCI DSS requirement explicitly as stated, due to legitimate and documented technical or business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. To understand the intent of a requirement, see the Customized Approach Objective for most PCI DSS requirements. If a requirement is not eligible for the Customized Approach and therefore does not have a Customized Approach Objective, refer to the Purpose in the Guidance column for that requirement.
3. Be “above and beyond” other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. When evaluating “above and beyond” for compensating controls, consider the following:

Note: All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS assessment. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a given compensating control will not be effective in all environments.

a. Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting cleartext administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of cleartext passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords). b. Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area but are not required for the item under review. c. Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to address a vulnerability that is exploitable through a network interface because a security update is not yet available from a vendor, a compensating control could consist of controls that include all of the following: 1) internal network segmentation, 2) limiting network access to the vulnerable interface to only required devices (IP address or MAC address filtering), and 3) IDS/IPS monitoring of all traffic destined to the vulnerable interface. 5. Address the additional risk imposed by not adhering to the PCI DSS requirement. 6. Address the requirement currently and in the future. A compensating control cannot address a requirement that was missed in the past (for example, where performance of a task was required two quarters ago, but that task was not performed). The assessor is required to

thoroughly evaluate compensating controls during each annual PCI DSS assessment to confirm that each compensating control adequately addresses the risk that the original PCI DSS requirement was designed to address, per items 1-6 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete. Additionally, compensating control results must be documented in the applicable report for the assessment (for example, a Report on Compliance or a Self-Assessment Questionnaire) in the corresponding PCI DSS requirement section, and included when the applicable report is submitted to the requesting organization.

appendices | principles | top

REQUIREMENTS and TESTING PROCEDURES x.y

DEFINED APPROACH REQUIREMENTS

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

DEFINED APPROACH TESTING PROCEDURES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

REQUIREMENTS and TESTING PROCEDURES x.y

DEFINED APPROACH REQUIREMENTS

CUSTOMIZED APPROACH OBJECTIVE

APPLICABILITY NOTES

GUIDANCE

Purpose

Good Practice

Definitions

Examples

Further Information

Section A3 | top

Annotations Requirement 1

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
1.1.1	Document Examination and Personnel Interview	Security policies and operational procedures documentation pertaining to Requirement 1.	1. Can you provide the documents outlining the security policies and operational procedures as mentioned in Requirement 1? 2. Can you explain how these policies and procedures are managed and followed in accordance with the specified elements in this requirement?
1.1.2.a	Document Examination	Documentation describing the roles and responsibilities for performing	1. Can you provide the document that details the roles and responsibilities

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		activities as specified in Requirement 1.	assigned for activities in Requirement 1? 2. How are these roles and responsibilities communicated within the organization?
1.1.2.b	Personnel Interview	Evidence of understanding of assigned roles and responsibilities by relevant personnel; it may include training records or meeting minutes.	1. Can you explain your role and responsibilities regarding activities in Requirement 1? 2. How were these roles and responsibilities communicated to you? 3. Can you provide examples of how you fulfill these responsibilities in your role?
1.2.1.a	Document Examination	Configuration standards documentation for NSC rulesets.	1. Can you provide the documentation that showcases the configuration standards for NSC rulesets in line with this requirement?
1.2.1.b	Document Examination	Documentation or system screenshots showing NSC ruleset configurations.	1. Can you demonstrate that the NSC rulesets are configured according to the documented standards?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
1.2.2.a	Document Examination	Documented procedures for changes in network connections and NSC configurations, aligned with Requirement 6.5.1.	1. Can you present the documented procedures that govern changes to network connections and NSC configurations?
1.2.2.b	Document Examination and Personnel Interview	Change control records and evidence of approval for network connection changes.	1. Can you provide records of approved and managed changes to network connections as per Requirement 6.5.1?
1.2.2.c	Document Examination and Personnel Interview	Change control records and evidence of approval for changes in NSC configurations.	1. Can you provide records of approved and managed changes to NSC configurations in accordance with Requirement 6.5.1?
1.2.3.a	Document Examination	Current network diagrams and network configuration documentation.	1. Can you provide the network diagrams that are in accordance with the elements specified in this requirement?
1.2.3.b	Document Examination and Personnel Interview	Documentation of network diagram updates and evidence of regular review by responsible personnel.	1. Can you demonstrate that the network diagrams are accurate and updated with changes in the environment?
1.2.4.a	Document Examination and Personnel Interview	Current data-flow diagrams	1. Can you present the data-flow

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		showcasing all account data flows.	diagrams which illustrate all account data flows as per this requirement?
1.2.4.b	Document Examination and Personnel Interview	Documentation of data-flow diagram updates and evidence of regular review by responsible personnel.	1. Can you demonstrate that the data-flow diagrams are accurate and updated with environmental changes?
1.2.5.a	Document Examination	Documentation listing all approved services, protocols, and ports with corresponding business justifications.	1. Can you present a document that lists all approved services, protocols, and ports, including the business justification for each?
1.2.5.b	Document Examination	NSC configuration settings verifying the use of only approved services, protocols, and ports.	1. Can you demonstrate that only approved services, protocols, and ports are in use as per the configurations?
1.2.6.a	Document Examination	Documentation identifying all insecure services, protocols, and ports in use with defined security features to mitigate risk.	1. Can you present documentation that identifies all insecure services, protocols, and ports and the defined security features for each?
1.2.6.b	Document Examination	NSC configuration settings demonstrating the	1. Can you demonstrate that the defined security

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		implementation of defined security features for identified insecure services, protocols, and ports.	features have been implemented for each identified insecure service, protocol, and port?
1.2.7.a	Document Examination	Documentation defining procedures for semi-annual reviews of NSC configurations.	1. Can you provide documentation that outlines procedures for reviewing NSC configurations at least every six months?
1.2.7.b	Document Examination and Personnel Interview	Documentation of reviews and interviews corroborating semi-annual reviews of NSC configurations.	1. Can you demonstrate that reviews of NSC configurations have occurred at least every six months through documented evidence?
	Document Examination**1.2.7.c**	NSC configurations demonstrating the removal or update of configurations not supported by business justification.	1. Can you provide evidence of configurations that were removed or updated due to lack of business justification?
1.2.8	Document Examination	Configuration files of NSCs that comply with this requirement.	1. Can you present NSC configuration files that are in accordance with all the elements specified in this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
1.3.1.a	Document Examination & Interview	NSC configuration standards documentation	1. Can you demonstrate how the configuration standards restrict inbound traffic to the CDE as specified in this requirement?
1.3.1.b	Document Examination & Observation	NSC configurations settings and logs	1. Can you provide evidence that the NSC configurations effectively restrict inbound traffic to the CDE in line with the specified standards?
1.3.2.a	Document Examination & Interview	NSC configuration standards documentation	1. Can you elucidate how the configuration standards restrict outbound traffic from the CDE as outlined in this requirement?
1.3.2.b	Document Examination & Observation	NSC configurations settings and logs	1. Can you provide evidence that the NSC configurations restrict outbound traffic from the CDE according to the specified standards?
1.3.3	Document Examination & Interview	NSC configuration settings and network diagrams	1. Can you show how NSCs are implemented between all wireless networks and the CDE, and demonstrate compliance with the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			specific elements mentioned in this requirement?
1.4.1.a	Document Examination & Interview	NSC configuration standards and network diagrams	1. Can you provide the configuration standards and network diagrams that outline the defined NSCs between trusted and untrusted networks?
1.4.1.b	Document Examination & Observation	Network configurations and NSC documentation	1. Can you showcase how the NSCs are implemented between trusted and untrusted networks as per the documented configuration standards and network diagrams?
1.4.2	Document Examination & Observation	Vendor documentation and NSC configurations	1. Can you demonstrate how inbound traffic from untrusted networks to trusted networks is restricted as detailed in this requirement?
1.4.3	Document Examination & Observation	Vendor documentation and NSC configurations	1. Can you elucidate on the anti-spoofing measures in place to detect and block forged source IP addresses from

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			entering the trusted network?
1.4.4.a	Document Examination	Data-flow diagram and network diagram	1. Can you verify from the data-flow and network diagrams that components storing cardholder data are not directly accessible from untrusted networks?
1.4.4.b	Document Examination & Observation	NSC configurations	1. Can you show the NSC configurations that ensure components storing cardholder data are not directly accessible from untrusted networks?
1.4.5.a	Document Examination & Observation	NSC configurations	1. Can you illustrate how the NSC configurations restrict the disclosure of internal IP addresses and routing information to only authorized parties?
1.4.5.b	Interview & Document Examination	Personnel interviews and policy documentation	1. Can you confirm the measures in place that restrict the disclosure of internal IP addresses and routing information to authorized parties only?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
1.5.1.a	Document Examination & Interview	Policies, configuration standards, and personnel interviews	1. Can you provide the policies and configuration standards that govern the security controls for computing devices connecting to both untrusted networks and the CDE? 2. Can you discuss how these controls are implemented in line with the stipulations of this requirement?
1.5.1.b	Document Examination & Observation	Configuration settings on the concerned computing devices	1. Can you show the configuration settings on computing devices that connect to both untrusted networks and the CDE? 2. Can you verify that these settings adhere to all the elements outlined in this requirement?

annotations 1 | annotations | requirements | principles | top

Annotations Requirement 2

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
2.1.1	Interview and document examination	Security policies and operational procedures documentation relating to Requirement 2	1. Can you provide the documentation that outlines the security policies and operational procedures identified in Requirement 2? 2. How are these policies and procedures managed and maintained in accordance with the elements specified in this requirement? 3. Can you demonstrate how these policies are communicated and adhered to within the organization?
2.1.2.a	Document examination	Documented descriptions of roles and responsibilities for performing activities in Requirement 2	1. Can you provide the documentation that delineates the roles and responsibilities for activities outlined in Requirement 2? 2. Are the descriptions of roles and responsibilities comprehensive and clear? 3. How are changes to roles and responsibilities documented and communicated?
2.1.2.b	Interview	Evidence of assignment and	1. Can you articulate your roles and

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		understanding of roles and responsibilities pertaining to activities in Requirement 2	responsibilities as they pertain to Requirement 2? 2. How were you informed of your roles and responsibilities? 3. Can you demonstrate an understanding of the actions to be taken in line with your roles and responsibilities?
2.2.1.a	Document Examination	System configuration standards documents	Can you show the system configuration standards and how they encompass all elements mentioned in this requirement?
2.2.1.b	Document Examination and Interview	Policies, procedures, and evidence of updates regarding vulnerability issues	How are the system configuration standards updated when new vulnerabilities are identified as per Requirement 6.3.1?
2.2.1.c	Document Examination and Interview	Evidence of configuration settings being applied during the configuration of new systems	Can you demonstrate that the system configuration standards are applied and verified when configuring new systems?
2.2.2.a	Document Examination	System configuration standards highlighting the management of vendor default accounts	How do your system configuration standards guide the management of vendor default accounts as per this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
2.2.2.b	Document Examination and Observation	Vendor documentation and observation of login process utilizing vendor default accounts	Can you demonstrate how vendor default accounts are implemented in accordance with this requirement?
2.2.2.c	Document Examination and Interview	Configuration files and evidence of the removal or disabling of unused vendor default accounts	Can you confirm that all unused vendor default accounts are either removed or disabled?
2.2.3.a	Document Examination	System configuration standards emphasizing the management of primary functions with varying security levels	How do the system configuration standards ensure the management of primary functions with differing security levels?
2.2.3.b	Document Examination	System configurations showing the management of primary functions with differing security levels	Can you show how primary functions with different security levels are managed according to this requirement?
2.2.3.c	Document Examination	System configurations in cases where virtualization technologies are used	How are functions with differing security levels managed on the same system component where virtualization technologies are used?
2.2.4.a	Document Examination	Documentation identifying and detailing necessary system services, protocols, and daemons	How are necessary system services, protocols, and daemons documented in your system configuration standards?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
2.2.4.b	Document Examination	System configurations showing the removal or disabling of unnecessary functionalities	Can you demonstrate that all unnecessary functionalities are removed or disabled and only required functionalities are enabled?
2.2.5.a	Document Examination and Interview	System configuration standards and personnel knowledge about the management of insecure services, protocols, or daemons	How are insecure services, protocols, or daemons managed and implemented according to this requirement?
2.2.5.b	Document Examination	Configuration settings showcasing additional security features implemented to mitigate risks associated with insecure services, protocols, or daemons	Can you display the security features in place to mitigate the risk of using insecure services, protocols, and daemons?
2.2.6.a	Document Examination	System configuration standards outlining the prevention of misuse through security parameters	How do the system configuration standards guide the setting up of system security parameters to prevent misuse?
2.2.6.b	Interview	Knowledge of system administrators/security managers regarding common security parameter settings	Can the system administrators/security managers explain the common security parameter settings for the system components?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
2.2.6.c	Document Examination	Evidence of appropriate setup of common security parameters in system configurations	Can you demonstrate that common security parameters are set appropriately according to the system configuration standards?
2.2.7.a	Document Examination	System configuration standards ensuring the encryption of non-console administrative access	How do your system configuration standards facilitate the encryption of all non-console administrative access using strong cryptography?
2.2.7.b	Observation and Document Examination	Observation of administrator login process and system configurations emphasizing secure non-console administrative access management	Can you demonstrate that non-console administrative access is managed according to this requirement?
2.2.7.c	Document Examination	Settings of system components and authentication services highlighting the unavailability of insecure remote login services	Can you confirm that insecure remote login services are not available for non-console administrative access?
2.2.7.d	Document Examination and Interview	Vendor documentation and personnel knowledge regarding the implementation of strong cryptography	Can you verify that strong cryptography is implemented according to industry best practices or vendor recommendations?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		as per industry best practices/vendor recommendations	
2.3.1.a	Document Examination and Interview	Policies, procedures and interviews with responsible personnel	Can you outline the processes defined for changing or securing wireless vendor defaults upon installation in line with this requirement?
2.3.1.b	Document Examination and Observation	Vendor documentation and observation of system administrator login process to wireless devices	Can you demonstrate that SNMP defaults and default passwords/passphrases on wireless access points are not used?
2.3.1.c	Document Examination	Vendor documentation and wireless configuration settings	Can you show any changes made to security-related wireless vendor defaults, if applicable?
2.3.2	Interview and Document Examination	Interviews with responsible personnel and key-management documentation	Can you confirm that wireless encryption keys are changed as specified in this requirement?

annotations 2 | annotations | requirements | principles | top

---

Annotations Requirement 3

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
3.1.1	Document Examination/Interview	Security policies and operational	1. Can you demonstrate how the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		procedures documented in Requirement 3	security policies are managed and maintained? 2. Have these policies been communicated and understood by the relevant personnel?
3.1.2.a	Document Examination	Documentation detailing the descriptions of roles and responsibilities pertaining to activities mentioned in Requirement 3	1. Can you show me the documentation where the roles and responsibilities are outlined for activities mentioned in Requirement 3? 2. Have the roles been assigned according to this documentation?
3.1.2.b	Interview	Confirmation from personnel regarding their roles and responsibilities	1. Can you explain your role and responsibilities in performing the activities detailed in Requirement 3? 2. Are these responsibilities well-understood and implemented accordingly?
3.2.1.a	Document Examination and Interview	Data retention and disposal policies, procedures, and processes	1. Can you explain the processes defined in the data retention and disposal policies? Are

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			all elements specified in this requirement included? 2. How are these policies communicated to the relevant personnel and how do you ensure adherence?
3.2.1.b	Document Examination	Files and system records on system components where account data is stored	1. Can you demonstrate that the data storage amount and retention time are in compliance with the defined data retention policy?
		Data retention policy	1. How is the data storage monitored to ensure compliance with the data retention policy?
3.2.1.c	Observation	Mechanisms used to render account data unrecoverable	1. Can you show the mechanisms in place to ensure account data cannot be recovered once it has been deleted? Are there any controls in place to verify the efficiency of these mechanisms?
3.3.1.a	Document Examination	Documented policies, procedures, and	1. Can you provide the documented policies and system

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		system configurations	configurations that ensure SAD is not retained post-authorization? 2. How do you ensure compliance with these policies and configurations?
3.3.1.b	Document Examination/Observation	Documented procedures and observations of secure data deletion processes	1. Can you demonstrate the secure data deletion processes in place to render SAD unrecoverable after authorization? 2. How are these processes monitored and validated?
3.3.1.1	Document Examination	Data sources	1. Can you verify that no full track data contents are stored post-authorization? 2. How is this verified and monitored on a regular basis?
3.3.1.2	Document Examination	Data sources	1. Can you verify that card verification codes are not stored after the authorization process? 2. How do you ensure compliance with this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
3.3.1.3	Document Examination	Data sources	1. Can you demonstrate that PINs and PIN blocks are not stored upon the completion of the authorization process? 2. How is the non-storage of this data monitored and ensured?
3.3.2	Document Examination	Data stores, system configurations, and/or vendor documentation	1. Can you demonstrate that all stored SAD is encrypted using strong cryptography before the completion of authorization? 2. How is the strength of the cryptography verified?
3.3.3.a	Document Examination/Interview	Documented policies and interviews with personnel	1. Is there documented business justification for storing sensitive authentication data? Can personnel explain these justifications? 2. How is the necessity for data storage periodically reviewed?
3.3.3.b	Document Examination	Data stores and system	1. Can you showcase how sensitive

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		configurations	authentication data is stored securely? 2. What measures are in place to ensure the security of stored data, especially concerning sensitive authentication data?
3.4.1.a	Document Examination	Policies and procedures for masking the display of PANs	1. Can you show the documented list of roles with access to more than the BIN and last four digits of the PAN, along with the legitimate business reasons? 2. Are there clear policies in place that detail the masking of PAN when displayed?
3.4.1.b	System Configuration Examination	System configurations	1. Can you provide evidence that system configurations only allow the display of full PAN for roles with a documented business need? 2. How are these configurations monitored and maintained?
3.4.1.c	Display Examination	Displays of PAN (on screen, on paper receipts)	1. Can you demonstrate that PANs are appropriately masked

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			on displays and only accessible by those with a legitimate business need? 2. What measures are in place to ensure this masking is enforced across various display mediums?
3.4.2.a	Document Examination	Policies, procedures, and evidence for technical controls regarding remote-access technologies	1. Can you show the documented policies and procedures that prevent unauthorized personnel from copying and/or relocating PAN? 2. Can you provide the list of personnel authorized to copy and/or relocate PAN, along with the documented authorizations and business needs?
3.4.2.b	System Configuration Examination	Configurations for remote-access technologies	1. Can you demonstrate the technical controls in place to prevent the unauthorized copying and/or relocating of PAN via remote-access technologies? 2. How are these

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			controls monitored and maintained?
3.4.2.c	Observation and Interview	Observations of processes and interviews with personnel	1. Can you show that only personnel with documented authorization and a legitimate business need are permitted to copy and/or relocate PAN using remote-access technologies? 2. How is compliance with this requirement monitored and enforced?
3.5.1.a	Document Examination	Documentation about the system rendering PAN unreadable including vendor, type, and encryption algorithms (if applicable)	1. Can you provide the documentation detailing the system used to render PAN unreadable, including details on the vendor, type of system/process, and encryption algorithms used?
3.5.1.b	Data and Logs Examination	Data repositories and audit logs including payment application logs	1. Can you show that PAN is rendered unreadable in data repositories and audit logs, in accordance with the specified methods in this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
3.5.1.c	Control Examination	Implemented controls over hashed and truncated versions of PAN	1. Can you demonstrate that controls are in place to prevent the correlation of hashed and truncated versions of PAN to reconstruct the original PAN?
3.5.1.1.a	Document Examination	Documentation on the hashing method, including vendor, type of system/process, and encryption algorithms (if applicable)	1. Can you provide documentation detailing the hashing method used for rendering PAN unreadable, including information on the vendor, system/process, and any encryption algorithms?
3.5.1.1.b	Document Examination	Documentation on key management procedures and processes related to cryptographic hashes	1. Can you show that key management processes and procedures are in compliance with Requirements 3.6 and 3.7, especially in relation to cryptographic hashes?
3.5.1.1.c	Data Repository Examination	Data repositories	1. Can you demonstrate that PAN data in repositories is

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			rendered unreadable as mandated?
3.5.1.1.d	Logs Examination	Audit logs including payment application logs	1. Can you confirm that the audit logs, including those in payment applications, show evidence of PAN being rendered unreadable?
3.5.1.2.a	Encryption Process Examination	Encryption processes documentation for disk-level or partition-level encryption	Can you verify that the encryption processes in place comply with the stipulations outlined in sub-requirement 3.5.1.2.a for rendering PAN unreadable?
3.5.1.2.b	Configuration and Process Observation	Configuration documentation and/or vendor documentation and observation of encryption processes	1. Can you demonstrate that the system configurations align with vendor documentation and effectively render disks or partitions unreadable?
3.5.1.3.a	System Configuration and Observation	System configuration documentation and observation of the authentication process	1. Can you verify that logical access, as outlined in this requirement, is correctly implemented when disk-level or partition-

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			level encryption is used?
3.5.1.3.b	File Examination and Personnel Interview	Files containing authentication factors and interviews with relevant personnel	1. Can you ensure that authentication factors granting access to unencrypted data are stored securely and independently from the OS's authentication and access control methods?
3.6.1	Document Examination	Documented key-management policies and procedures	1. Can you provide the documented policies and procedures that detail the protection processes for cryptographic keys used to safeguard stored account data?
3.6.1.1	Personnel Interview & Document Examination	Documentation describing the cryptographic architecture (for service providers)	1. Can you present a document that describes the cryptographic architecture, including all the elements specified in this requirement? (Service provider assessments only)
3.6.1.2.a	Document Examination	Documented procedures on	1. Can you show the documented

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		forms of cryptographic keys	procedures that define the allowable forms of cryptographic keys used to encrypt/decrypt stored account data?
3.6.1.2.b	System Configuration Examination	System configurations and key storage locations	1. Can you demonstrate that cryptographic keys used to encrypt/decrypt stored account data exist only in the forms specified in this requirement, as verified by system configurations and key storage locations?
3.6.1.2.c	System Configuration Examination	System configurations and key storage locations for key-encrypting keys	1. Can you confirm that: The key-encrypting keys are at least as strong as the data-encrypting keys they protect? Key-encrypting keys are stored separately from data-encrypting keys?
3.6.1.3	User Access List Examination	User access lists	1. Can you provide user access lists that show restricted access to cleartext

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			cryptographic key components, limited to the fewest number of custodians necessary?
3.6.1.4	Process Observation & Location Examination	Key storage locations and processes	1. Can you demonstrate that keys are stored in the minimum possible number of locations, as observed through key storage locations and processes?

annotations 3 | annotations | requirements | principles | top

Annotations Requirement 4

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
4.1.1	Document Examination and Personnel Interview	- Security policies pertaining to Requirement 4. - Operational procedures identified in Requirement 4.	1. Can you provide the security policies identified for Requirement 4? 2. How are these operational procedures managed and maintained? 3. How often are these policies and procedures reviewed and up**dated?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
4.1.2.a	Document Examination	- Descriptions of roles and responsibilities for activities under Requirement 4. - Documents assigning these roles and responsibilities.	1. Can you present the documentation where the roles and responsibilities for Requirement 4 are defined? 2. Are these roles and responsibilities clearly assigned to specific personnel or teams? 3. How is the alignment with these documented responsibilities verified?
4.1.2.b	Personnel Interview	- Records of personnel being assigned specific roles and responsibilities as per Requirement 4. - Evidence of understanding these roles and responsibilities by the personnel.	1. Can you elaborate on the roles and responsibilities assigned to you as part of Requirement 4? 2. How were you informed or trained about your roles and responsibilities? 3. Can you demonstrate a situation where you had to perform activities as per your assigned role under Requirement 4?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
4.2.1.a	Document Examination and Personnel Interview	- Documented policies and procedures specifying processes under this requirement. - Records of interviews with personnel responsible for these processes.	1. Can you show the documented processes as per this requirement? 2. How are personnel made aware of these processes? 3. Can you illustrate how these processes are implemented in practice?
4.2.1.b	System Configurations Examination	System configuration documents showing implementation of strong cryptography and security protocols.	1. Can you provide evidence of the implemented strong cryptography and security protocols? 2. How are these configurations maintained and updated to ensure data security?
4.2.1.c	Cardholder Data Transmission Examination	Records of cardholder data transmissions showing the encryption of PAN using strong cryptography.	1. Can you demonstrate how PAN is encrypted during transmission over open, public networks? 2. How do you ensure the encryption method used is strong and up-to-date?
4.2.1.d	System Configurations Examination	System configuration documents showing	1. Can you show how the system

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		the rejection of unverified keys/certificates.	rejects keys or certificates that cannot be verified as trusted? 2. What mechanisms are in place to maintain trust with utilized keys and certificates?
4.2.1.1.a	Document Examination	Documented policies and procedures on maintaining an inventory of trusted keys and certificates.	1. Can you provide the documented policies and procedures for maintaining an inventory of trusted keys and certificates? 2. How is the inventory maintained and updated?
4.2.1.1.b	Inventory Examination	The latest inventory of trusted keys and certificates.	1. Can you show the current inventory of trusted keys and certificates? 2. How frequently is this inventory updated?
4.2.1.2	System Configurations Examination	System configuration documents illustrating the use of strong cryptography for wireless network authentication and transmission.	1. Can you demonstrate the implementation of industry best practices for strong cryptography in wireless networks? 2. How do you

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			ensure that the wireless networks connected to the CDE adhere to these standards?
4.2.2.a	Document Examination	Documented policies and procedures outlining the processes to secure PAN with strong cryptography for end-user messaging technologies.	1. Can you provide the policies and procedures for securing PAN sent over end-user messaging technologies? 2. How are these processes implemented and maintained?
4.2.2.b	System Configurations and Vendor Documentation Examination	System configuration documents and vendor documentation showing the securing of PAN with strong cryptography for end-user messaging technologies.	1. Can you demonstrate the system configurations that secure PAN during transmission via end-user messaging technologies? 2. How do you verify that the cryptography applied is robust and secure?

annotations 4 | annotations | requirements | principles | top

Annotations Requirement 5

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
5.1.1	Documentation examination and personnel interview	Security policies and operational procedures identified in Requirement 5	1. Can you provide the security policies that align with Requirement 5? 2. Can you explain how these policies are managed in accordance with the stipulated elements?
5.1.2.a	Documentation examination	Descriptions of roles and responsibilities documented and assigned for Requirement 5 activities	1. Can you showcase the documented descriptions of roles and responsibilities for Requirement 5? 2. How are these roles assigned and documented?
5.1.2.b	Personnel interview	Confirmation that roles and responsibilities are understood and assigned as documented for Requirement 5	1. Can you explain your role and responsibilities concerning Requirement 5? 2. How do you ensure these responsibilities are understood and followed?
5.2.1.a	System components examination	Evidence of anti-malware solution deployed on all applicable system components	1. Can you demonstrate how the anti-malware solution is deployed on all system components and how it has been assessed for risk

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			according to Requirement 5.2.3?
5.2.1.b	Periodic evaluations documentation examination	Records of periodic evaluations indicating components not at risk from malware	1. Can you provide the periodic evaluations where it was determined that certain system components are not at risk from malware?
5.2.2	Vendor documentation and configurations examination	Vendor documentation and configurations showcasing malware detection, removal, blocking or containment features	1. Can you showcase how the anti-malware solution detects, removes, blocks or contains all known types of malware as per vendor documentation?
5.2.3.a	Policies and procedures documentation examination	Documented policies and procedures for periodic evaluations	1. Can you provide the documented policies and procedures for conducting periodic evaluations as specified in this requirement?
5.2.3.b	Personnel interview	Testimonies confirming adherence to defined evaluation procedures	1. Can you explain the process followed during periodic evaluations and confirm that all specified elements are included?
5.2.3.c	System components list examination	A matching list of system components	1. Can you verify that the system

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		from requirements 5.2.1 and 5.2.3	components identified as not at risk match with those listed under Requirement 5.2.1?
5.2.3.1.a	Risk analysis documentation examination	Targeted risk analysis documents in line with Requirement 12.3.1	1. Can you provide the targeted risk analysis performed in accordance with Requirement 12.3.1 for evaluating system components?
5.2.3.1.b	Periodic evaluations documentation and personnel interview	Documented results of periodic evaluations and interview confirmations	1. Can you confirm the frequency of the periodic evaluations as defined in the targeted risk analysis, and present the documented results?
5.3.1.a	Anti-malware configurations examination	Configurations showing automatic updates setup	1. Can you show the configurations of the anti-malware solutions indicating the setup for automatic updates?
5.3.1.b	System components and logs examination	Logs indicating current and promptly deployed anti-malware definitions	1. Can you provide the logs that confirm the anti-malware solutions and definitions are up to date and deployed promptly?
5.3.2.a	Anti-malware configurations	Configuration details indicating	1. Can you showcase the anti-malware

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
	examination	fulfillment of at least one specified element	solutions configurations meeting at least one of the specified elements in this requirement?
5.3.2.b	System components examination	Evidence that solution is enabled in line with at least one specified element for operating systems at risk	1. Can you confirm that the solution is enabled and configured in accordance with the specified elements for systems at risk of malware?
5.3.2.c	Logs and scan results examination	Logs and scan results confirming the solution's enablement as per specified elements	1. Can you provide the logs and scan results that verify the anti-malware solution is enabled as per the specified requirements?
5.3.2.1.a	Risk analysis documentation examination	Targeted risk analysis documents as per Requirement 12.3.1	1. Can you showcase the targeted risk analysis done for determining the frequency of malware scans in line with Requirement 12.3.1?
5.3.2.1.b	Documentation and personnel interview	Documented results of periodic malware scans and interview confirmations	1. Can you present the documented results of periodic malware scans and confirm the frequency defined in the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			targeted risk analysis?
5.3.3.a	Anti-malware configurations examination	Configurations showcasing protections for removable electronic media	1. Can you demonstrate how the anti-malware solution is configured to protect removable electronic media as specified in this requirement?
5.3.3.b	System components examination	Evidence of solution enablement on systems with connected removable electronic media	1. Can you verify that the solution is enabled on system components with connected removable electronic media as specified in this requirement?
5.3.3.c	Logs and scan results examination	Logs and scan results demonstrating solution's effectiveness on removable electronic media	1. Can you provide logs and scan results that confirm the anti-malware solution's enablement and effectiveness on removable electronic media?
5.3.4	Anti-malware configurations examination	Configurations indicating log enablement and retention as per Requirement 10.5.1	1. Can you show that the anti-malware solution configurations enable and retain logs as mandated by Requirement 10.5.1?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
5.3.5.a	Anti-malware configurations examination	Configurations indicating restrictions on altering or disabling anti-malware mechanisms	1. Can you verify that the anti-malware mechanisms cannot be altered or disabled by users through the configuration settings?
5.3.5.b	Personnel interview and process observation	Documented and authorized requests for temporary disabling or alteration of anti-malware mechanisms	1. Can you confirm that any requests to alter or disable anti-malware mechanisms are documented and authorized by management? How is this process managed?
5.4.1	Process and mechanism observation	Observation and mechanisms confirming controls against phishing attacks	1. Can you demonstrate the controls in place to detect and protect personnel against phishing attacks?

annotations 5 | annotations | requirements | principles | top

---

Annotations Requirement 6

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
** 6.1.1**	Document Examination and Personnel Interview	- Security policies and operational procedures concerning Requirement 6	1. Can you provide the documentation that details the security policies and operational

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		- Evidence of policy management & compliance tracking	procedures as mentioned in Requirement 6? 2. How are these policies managed and tracked within the organization? 3. How is compliance with these policies ensured and monitored?
6.1.2.a	Document Examination	- Descriptions of roles and responsibilities regarding activities in Requirement 6 - Assignment of roles and responsibilities	1. Can you provide documentation that outlines the roles and responsibilities assigned for performing activities related to Requirement 6? 2. How are these roles and responsibilities communicated within the organization?
6.1.2.b	Personnel Interview	- Evidence of understanding roles and responsibilities among assigned personnel - Training and awareness materials	1. Can you describe your role and responsibilities concerning Requirement 6? 2. How were you informed or trained about your responsibilities? 3. How do you

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			ensure that the roles and responsibilities are effectively executed as documented?
6.2.1	Document Examination	Documented software development procedures which encompass all elements stated in the requirement	1. Can you provide the documented procedures for software development that align with the stipulations of this requirement?
6.2.2.a	Document Examination	Software development procedures defining training processes for personnel involved in developing bespoke and custom software	1. Can you show the documented processes defined for training software development personnel in developing custom software?
6.2.2.b	Document Examination and Personnel Interview	Training records indicating the coverage of relevant software security training, aligned with job functions and development languages	1. Can you showcase the training records for personnel involved in bespoke and custom software development? 2. How is the relevance of the training to job functions ensured?
6.2.3.a	Document Examination and Personnel Interview	Documented software development	1. Can you illustrate the defined processes for

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		procedures highlighting processes for reviewing bespoke and custom software	reviewing custom software as documented in your development procedures?
6.2.3.b	Document Examination	Evidence of changes to bespoke and custom software being reviewed as per the stipulated requirements	1. Could you present evidence demonstrating the review process of code changes in accordance with the specified requirement?
6.2.3.1.a	Document Examination and Personnel Interview	Documented software development procedures and interviews substantiating the definition of processes for manual code reviews	1. Can you describe the processes defined for conducting manual code reviews before releasing the software to production?
6.2.3.1.b	Document Examination and Personnel Interview	Evidence of manual code reviews being conducted as defined, and personnel testimonials to verify the process	1. Can you show evidence of manual code reviews conducted for bespoke and custom software? 2. Can personnel verify adherence to these procedures?
6.2.4	Document Examination and Personnel Interview	Documented procedures and testimonials from software	1. Can you demonstrate the procedures and techniques

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		development personnel, verifying the use of defined methods to counter common attacks	implemented to prevent or mitigate common software attacks in custom software development?
6.3.1.a	Document Examination	Policies and procedures documents detailing the processes for identifying and managing security vulnerabilities as per the stipulations of this requirement	1. Can you provide the existing policies and procedures that delineate the process of identifying and managing security vulnerabilities in line with the directives of this requirement?
6.3.1.b	Personnel Interview and Process Observation	Interviews and observation records verifying the management of security vulnerabilities as detailed in the defined processes	1. Could you elucidate how the processes are followed to identify and manage security vulnerabilities as specified? 2. Can you show documentation to substantiate adherence to these processes?
6.3.2.a	Document Examination and Personnel Interview	Documentation showcasing an inventory of bespoke and custom software along with third-party components incorporated into	1. Can you present the maintained inventory of custom and third-party software components? 2. How is this

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		them, and interviews verifying the usage of this inventory to identify and manage vulnerabilities	inventory utilized to identify and address vulnerabilities?
6.3.2.b	Document Examination	Software documentation corroborating the inclusion of bespoke and custom software and third-party components in the inventory	1. Could you show the documentation for bespoke and custom software and how it aligns with the inventory? 2. How is the inventory updated with third-party software components data?
6.3.3.a	Document Examination	Policies and procedures specifying the processes for addressing vulnerabilities through the installation of pertinent security patches/updates	1. Can you delineate the defined processes for addressing vulnerabilities by installing relevant security patches or updates as mentioned in this requirement?
6.3.3.b	Document Examination and System Observation	List of installed security patches/updates on system components and corresponding documentation confirming compliance with the recent security	1. Can you present the current list of installed security patches or updates? 2. How do you ensure that the installations are up-to-date with the most recent security

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		patch/update information	patch/update information?
6.4.1	Document Examination, Personnel Interview, Record Examination	1. Documented processes relating to vulnerability security assessment tools or methods. 2. Records of application security assessments. 3. System configuration settings and audit logs.	1. Can you walk me through the processes documented for security assessment of public-facing web applications? 2. How are identified vulnerabilities managed and rectified?
	OR		
	System Configuration Examination, Audit Log Review, Personnel Interview	1. System configuration settings validating the installation of automated technical solutions. 2. Audit logs indicating the operation of the solution. 3. Interviews confirming the setup.	1. Can you show the system configurations that validate the installation of automated technical solutions? 2. How does the solution detect and prevent web-based attacks continuously?
6.4.2	System Configuration Examination, Audit Log Review, Personnel Interview	1. System configuration settings for the deployed automated solution. 2. Audit logs demonstrating the detection and prevention of web-based attacks.	1. Can you provide an overview of the automated solution in place for detecting and preventing web-based attacks? 2. How are the system configuration

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		3. Interviews with the responsible personnel.	settings configured to facilitate this?
6.4.3.a	Document Examination	Policies and procedures outlining the management of payment page scripts.	1. Could you present the policies and procedures that govern the management of payment page scripts? 2. How are these scripts managed in line with the stipulations of this requirement?
6.4.3.b	Personnel Interview, Record Examination, System Configuration Review	1. Interviews verifying the management of payment page scripts. 2. Inventory records and system configurations that document the management of payment page scripts.	1. Can you elucidate how payment page scripts are managed as per the defined processes? 2. Could you show the inventory records and system configurations pertaining to payment page script management?
6.5.1.a	Document Examination	Change control procedures documentation.	1. Can you provide the documented procedures for change controls pertaining to all system components in the production environment?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
6.5.1.b	Document Examination and Trace Analysis	Recent changes documentation and related change control documentation.	1. Can you showcase how recent changes have been documented and how they align with the established change control procedures?
6.5.2	Document Examination, Personnel Interview, Observation	Documentation for significant changes and interviews with relevant personnel.	1. How do you ensure that PCI DSS requirements are upheld during system or network changes? 2. Can you provide documentation supporting this?
6.5.3.a	Document Examination	Policies and procedures governing pre-production and production environment separation.	1. Can you detail the policies and procedures that dictate the separation of pre-production and production environments?
6.5.3.b	Document and Configuration Examination	Network documentation and configurations of network security controls.	1. How do you ensure that the network configuration enforces the separation between pre-production and production environments? 2. Can you provide

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			the relevant documentation?
6.5.3.c	Configuration Examination	Access control settings documentation.	1. Can you showcase the access control settings that enforce separation between the pre-production and production environments?
6.5.4.a	Document Examination	Policies and procedures for role and function separation during change deployment.	1. What policies and procedures are in place to separate roles and functions during the deployment of changes?
6.5.4.b	Process Observation, Personnel Interview	Observations of the process and interviews confirming role separation during deployment.	1. How are the roles and functions separated in practice during change deployment? 2. Can you provide examples or demonstrations?
6.5.5.a	Document Examination	Policies and procedures concerning the use of live PANs in pre-production environments.	1. What measures are defined to prevent the use of live PANs in pre-production environments, except for stipulated exceptions?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
6.5.5.b	Process Observation, Personnel Interview	Observations and interviews validating the non-use of live PANs in pre-production environments.	1. How do you ensure that live PANs are not used in pre-production environments, except where specified? 2. Can you provide evidence or examples?
6.5.5.c	Data Examination	Examination of pre-production test data to confirm the non-use of live PANs.	1. Can you showcase the pre-production test data to confirm that live PANs are not utilized, except where specified?
6.5.6.a	Document Examination	Policies and procedures for the removal of test data and accounts before production deployment.	1. What procedures are in place for the removal of test data and accounts before systems move into production?
6.5.6.b	Process Observation, Personnel Interview	Observations and interviews confirming the removal of test data and accounts before production.	1. Can you demonstrate the process of removing test data and accounts before transitioning systems to production?
6.5.6.c	Data and Account Examination	Data and account evaluations to confirm the absence of test data or	1. Can you provide evidence that there are no test data or accounts present in

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		accounts in production systems.	the production systems, especially for recently installed or updated software?

annotations 6 | annotations | requirements | principles | top

Annotations Requirement 7

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
7.1.1	Documentation Examination and Personnel Interview	Security policies and operational procedures pertaining to Requirement 7	1. Can you provide the documentation that outlines the security policies and operational procedures identified in Requirement 7? 2. How are these policies and procedures managed and maintained within the organization? 3. Can you demonstrate how access controls are implemented according to the policies outlined in Requirement 7?
7.1.2.a	Documentation Examination	Documentation detailing the descriptions of roles and responsibilities	1. Can you provide the documentation that outlines the roles and

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		for activities in Requirement 7	responsibilities for activities pertaining to Requirement 7? 2. How are these roles and responsibilities assigned and documented within the organization? 3. How do these roles contribute to maintaining the access control measures specified in Requirement 7?
7.1.2.b	Personnel Interview	Interviews with personnel responsible for activities in Requirement 7	1. Can you describe your role and responsibilities regarding activities in Requirement 7? 2. How were you informed about your responsibilities in relation to Requirement 7? 3. Can you illustrate how your role contributes to fulfilling the requirements specified in Requirement 7?
7.2.1.a	Documentation Examination & Personnel Interview	Documented policies and procedures defining the access control model	1. Could you provide the documented policies and procedures that

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			define your access control model? 2. How is the access control model aligned with the defined elements in this requirement?
7.2.1.b	Documentation & Settings Examination	Access control model settings documentation	1. Can you showcase how the access needs are defined in the access control model settings? 2. How do these settings adhere to the specified elements in this requirement?
7.2.2.a	Documentation Examination	Policies and procedures on assigning access to users	1. Could you provide the policies and procedures that detail the process of assigning access to users? 2. How are these policies ensuring compliance with the specified elements in this requirement?
7.2.2.b	Documentation Examination & Personnel Interview	User access settings documentation including for privileged users	1. Can you demonstrate the privileges assigned to users, especially privileged users? 2. How do management

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			personnel ensure that assigned privileges align with the specified elements in this requirement?
7.2.2.c	Personnel Interview	Interviews with personnel responsible for assigning access	1. Could you explain the process of assigning access to privileged users? 2. How do you ensure the process complies with the specified elements in this requirement?
7.2.3.a	Documentation Examination	Policies and procedures detailing privilege approval processes	1. Could you provide the policies and procedures that outline the process for privilege approvals? 2. How do these policies facilitate approval by authorized personnel in accordance with this requirement?
7.2.3.b	Documentation Examination	User IDs and assigned privileges documentation, documented approvals	1. Can you show the documented approvals for assigned privileges? 2. How do you ensure that the specified privileges match the roles

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			assigned to individuals?
7.2.4.a	Documentation Examination	Policies and procedures detailing user account and access privilege reviews	1. Could you provide the policies and procedures for reviewing user accounts and access privileges? 2. How do these policies ensure compliance with the elements specified in this requirement?
7.2.4.b	Personnel Interview & Documentation Examination	Periodic review results of user accounts	1. Could you provide the results of the most recent periodic reviews of user accounts? 2. How do these reviews ensure alignment with the specified elements in this requirement?
7.2.5.a	Documentation Examination	Policies and procedures detailing the management of system and application accounts and access privileges	1. Can you present the policies and procedures for managing and assigning access privileges to system and application accounts? 2. How do these policies comply with the elements specified in this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
7.2.5.b	Documentation Examination & Personnel Interview	Documentation of system and application account privileges, interviews with responsible personnel	1. Can you demonstrate how system and application account privileges are assigned and managed? 2. How do these practices align with the elements specified in this requirement?
7.2.5.1.a	Documentation Examination	Policies and procedures for reviewing application and system accounts and access privileges	1. Can you provide the policies and procedures for reviewing application and system accounts and access privileges? 2. How are these policies ensuring compliance with the elements specified in this requirement?
7.2.5.1.b	Risk Analysis Examination	Risk analysis documentation concerning the frequency of periodic reviews	1. Could you show the targeted risk analysis for determining the frequency of reviews for application and system accounts and privileges? 2. How was this analysis conducted in accordance with Requirement 12.3.1?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
7.2.5.1.c	Personnel Interview & Documentation Examination	Results of periodic reviews of system and application accounts and privileges	1. Can you provide the results of the most recent reviews of system and application accounts and privileges? 2. How do these reviews adhere to the elements specified in this requirement?
7.2.6.a	Documentation Examination & Personnel Interview	Policies and procedures on granting user access to query repositories of stored cardholder data	1. Could you provide the policies and procedures for granting user access to query repositories storing cardholder data? 2. How do these processes comply with the elements specified in this requirement?
7.2.6.b	Configuration Settings Examination	Configuration settings documentation for querying repositories of stored cardholder data	1. Can you demonstrate the configuration settings used for querying repositories of stored cardholder data? 2. How do these settings ensure compliance with the elements specified in this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
7.3.1	Document Examination and System Settings Inspection	Vendor documentation, system settings detailing access control mechanisms	1. Can you show how the access control system restricts access based on a user's need to know for each system component? 2. Can you provide documentation that outlines how access is managed across all system components?
7.3.2	Document Examination and System Settings Inspection	Vendor documentation, system settings displaying permissions based on job classification & function	1. Can you demonstrate how the access control system enforces permissions based on job classification and function? 2. Can you provide examples of how permissions are assigned to individuals, applications, and systems in alignment with their roles?
7.3.3	Document Examination and System Settings Inspection	Vendor documentation, system settings showcasing the "deny all" default setting	1. Can you show the system settings where the access control system is set to "deny all" by default? 2. How does the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			organization ensure that the "deny all" default setting is maintained and effectively implemented?

annotations 7 | annotations | requirements | principles | top

Annotations Requirement 8

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
8.1.1	Documentation Examination & Personnel Interview	Security policies and operational procedures documentation that relates to Requirement 8	1. Can you provide the security policies and operational procedures that are in accordance with Requirement 8? 2. How are these policies and procedures managed and maintained over time? 3. Can you demonstrate how accountability for actions performed is established through these policies?
8.1.2.a	Documentation Examination	Documented descriptions of roles and responsibilities concerning activities in Requirement 8	1. Can you show the documentation where the roles and responsibilities for Requirement 8 activities are described and assigned? 2. How are these roles and responsibilities communicated to

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			relevant personnel? 3. Can you identify any recent updates or changes to the roles and responsibilities documented?
8.1.2.b	Personnel Interview	Records of personnel having understanding and acknowledgment of their roles and responsibilities as documented	1. Can you explain your role and responsibilities in regards to Requirement 8 activities? 2. How were you informed of your roles and responsibilities? 3. Can you provide any evidence of training or acknowledgment of understanding your roles and responsibilities concerning Requirement 8?
8.2.1.a	Personnel Interview	Records of unique IDs assigned to each user for system components and cardholder data access	1. How are unique IDs assigned to each user? 2. Can you demonstrate the process?
8.2.1.b	Documentation Examination	Audit logs showcasing unique identifiers linked to individual users	1. Can you provide the audit logs that show unique identification for individuals accessing system components?
8.2.2.a	Documentation Examination	User account lists and relevant documentation showcasing the usage of shared authentication credentials	1. How are shared authentication credentials managed? Are they used on a

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			necessary and exception basis?
8.2.2.b	Documentation Examination	Authentication policies and procedures documentation	1. Can you show the processes defined for the usage of shared authentication credentials in the policy documents?
8.2.2.c	System Administrators Interview	Records of the management of shared authentication credentials	1. Can system administrators verify and explain the conditions under which shared authentication credentials are used?
8.2.3	Documentation Examination & Personnel Interview	Authentication policies and procedures and testimonies from personnel	1. Can you demonstrate that unique authentication factors are used for remote access to each customer premises?
8.2.4	Documentation Examination & System Setting Review	Documented authorizations and system settings across different account lifecycle phases	1. Can you show the documentation and system settings that ensure proper management of account lifecycles?
8.2.5.a	Documentation Examination	Information sources for terminated users and current user access lists	1. Can you provide evidence of deactivated or removed IDs for terminated users from the access lists?
8.2.5.b	Personnel Interview	Records of returned or deactivated physical authentication factors for terminated users	1. How is the return or deactivation of physical authentication factors for terminated users

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			managed and documented?
8.2.6	Documentation Examination & Personnel Interview	User accounts and last logon information and records	1. Can you show the measures in place to remove or disable inactive user accounts within 90 days of inactivity?
8.2.7	Documentation Examination & Personnel Interview	Documentation for managing accounts and evidence of adherence to stipulated elements	1. Can you provide documentation and evidence that third-party remote access accounts are managed according to the requirements?
8.2.8	System Configuration Examination	System configuration settings showcasing the session idle timeout features	1. Can you demonstrate that the system/session idle timeout features have been set to 15 minutes or less?
8.3.1.a	Document Examination	Documentation detailing the authentication factors used.	1. Can you provide the documentation that describes the authentication factor(s) utilized for user access to system components?
8.3.1.b	Observation	Demonstrations of various types of authentications across different system components.	1. Can you demonstrate how the authentication functions consistently with the documented authentication factor(s)?
8.3.2.a	Document and System Examination	Vendor documentation and system configuration settings.	1. Can you showcase the documentation and settings that ensure authentication factors are encrypted both during

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			transmission and storage?
8.3.2.b	System Examination	Authentication factor repositories.	1. How are the authentication factors stored securely to ensure unreadability?
8.3.2.c	System Examination	Data transmission logs and configurations.	1. Can you demonstrate how authentication factors are rendered unreadable during transmission?
8.3.3	Document Examination and Observation	Procedures for modifying authentication factors and evidence of user identity verification before modification.	1. How do you ensure that a user's identity is verified before allowing modification to their authentication factors?
8.3.4.a	System Examination	System configuration settings regarding account lockout parameters.	1. How is the system configured to lock out user accounts after a defined number of invalid logon attempts?
8.3.4.b	System Examination	System configuration settings for account lockout durations.	1. Can you show the system settings that dictate the lockout duration or the identity verification process to unlock?
8.3.5	Document Examination and Observation	Password/passphrase setting and resetting procedures and demonstrations of the same.	1. Can you provide the procedures followed for setting and resetting passwords/passphrases, and can this be demonstrated?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
8.3.6	System Examination	System configuration settings for password/passphrase complexity.	1. Can you demonstrate how the system enforces password/passphrase complexity as per the specified parameters?
8.3.7	System Examination	System settings for password/passphrase history.	1. How does the system ensure that new passwords/passphrases are not repeated within a certain history length?
8.3.8.a	Document Examination and Interview	Authentication policies and procedures and evidence of distribution to users.	1. How are the authentication policies and procedures distributed to all users and can you provide a copy of the same?
8.3.8.b	Document Examination	Copies of distributed authentication policies and procedures.	1. Can you show that the distributed authentication policies and procedures encompass all specified elements?
8.3.8.c	Interview	User testimonials.	1. How familiar are users with the established authentication policies and procedures?
8.3.9	System Examination	System configuration settings for managing passwords/passphrases when used as the sole authentication factor.	1. Can you detail how passwords/passphrases are managed when used as the only authentication factor in accordance with specified elements?
8.3.10 & **8.3.10.1**	Document and System Examination (Service	Guidance provided to customer users and system configuration	1. How are passwords/passphrases managed for customer

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
	provider assessments only)	settings for password/passphrase management.	user access, and is the guidance inclusive of all specified elements?
8.3.11.a	Document Examination	Authentication policies and procedures pertaining to physical security tokens, smart cards, and certificates.	1. Can you provide the procedures for utilizing physical security tokens, smart cards, and certificates?
8.3.11.b	Interview	Security personnel testimonials.	1. How do you ensure authentication factors are assigned to individual users and are not shared?
8.3.11.c	System Examination and/or Observation	System configuration settings and physical controls for authentication factor utilization.	1. Can you demonstrate the controls implemented to ensure only the intended user can utilize an authentication factor to gain access?
8.4.1.a	Document Examination & Observation	Network and system configurations detailing the MFA requirements for non-console administrative access into the CDE.	1. Can you provide the configuration files that specify the MFA requirements for non-console administrative access? 2. How do you ensure that MFA is enforced for all non-console access into the CDE?
8.4.1.b	Observation	Evidence of administrator personnel logging into the CDE utilizing MFA (log files, screenshots).	1. Can you demonstrate an instance where MFA is required for an administrator logging into the CDE? 2. How are MFA

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			authentications logged and monitored?
8.4.2.a	Document Examination & Observation	Network and system configurations that indicate the implementation of MFA for all access points into the CDE.	1. Can you provide documentation that demonstrates MFA implementation for all access points into the CDE? 2. How is this configuration maintained and audited?
8.4.2.b	Observation	Evidence showing personnel logging into the CDE using MFA (log files, screenshots).	1. Can you demonstrate a live instance where MFA is required for personnel logging into the CDE? 2. How is adherence to MFA policies ensured?
8.4.3.a	Document Examination & Observation	Network and system configurations for remote access servers, demonstrating MFA implementation as per the specified requirement.	1. Can you provide the configurations that verify MFA is implemented for remote access servers? 2. How do these configurations align with the elements specified in the requirement?
8.4.3.b	Observation	Evidence of personnel connecting remotely and utilizing MFA (logs of remote access connections, video demonstrations).	1. Can you demonstrate a scenario where personnel connecting remotely are required to use MFA? 2. How is the usage of MFA monitored for remote connections?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
8.5.1.a	Document Examination	Vendor system documentation highlighting the MFA system's resistance to replay attacks.	1. Can you provide vendor documentation that illustrates the MFA system's resilience against replay attacks? 2. How does the MFA system prevent replay attacks?
8.5.1.b	Document Examination	System configurations showcasing the appropriate setup of the MFA implementation in line with the mentioned requirement.	1. Could you provide the system configuration documents for the MFA implementation? 2. How do these configurations ensure adherence to the specifications mentioned in the requirement?
8.5.1.c	Interview & Observation	Documented instances of requests to bypass MFA along with the respective managerial approvals and time limitations.	1. Could you discuss the process undertaken to grant exceptions for MFA bypass requests? 2. Can you provide examples of documented and authorized requests to bypass MFA for a limited time period?
8.5.1.d	Observation	Observational evidence (e.g., video recordings, log files) of personnel logging into system components in the CDE, showcasing the necessity of successful authentication factors for access.	1. Can you demonstrate the process of logging into system components within the CDE? 2. How does the system ensure that access is granted only upon successful authentication across all factors?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
8.5.1.e	Observation	Observational evidence (e.g., video recordings, log files) of personnel connecting remotely, emphasizing the requirement of successful authentication across all factors for access.	1. Can you showcase the procedure for remote connection to the network? 2. How does the system confirm that access is only granted upon successful authentication of all factors?
8.6.1	Document Examination & Personnel Interview	Application and system account documentation, Interviews with administrative personnel.	1. Can you show how the application and system accounts are managed? 2. Can you demonstrate compliance with all elements specified in this requirement?
8.6.2.a	Personnel Interview & Document Examination	System development procedures documentation, Interviews with personnel involved in system development.	1. Can you describe the process for defining access parameters for interactive logins? 2. How do you ensure passwords/passphrases are not hardcoded in scripts or files?
8.6.2.b	Document Examination	Scripts, configuration/property files, bespoke and custom source code documentation.	1. Can you provide scripts, files, or source code for examination? 2. How do you verify that passwords/passphrases are not hardcoded in these resources?
8.6.3.a	Document Examination	Policies and procedures documentation focusing on the protection of passwords/passphrases.	1. How are procedures defined to protect passwords/passphrases from misuse?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			2. Can you show the documentation supporting this?
8.6.3.b	Document Examination	Risk analysis documentation including change frequency and complexity for passwords/passphrases.	1. Could you provide the risk analysis documentation regarding the change frequency and complexity of passwords/passphrases? 2. How does it align with the elements specified in Requirement 12.3.1?
8.6.3.c	Personnel Interview & Document Examination	Interviews with responsible personnel and system configuration settings documentation.	1. How are passwords/passphrases protected against misuse as per the specified elements in this requirement? 2. Can you provide documentation and setting configurations that demonstrate this?

annotations 8 | annotations | requirements | principles | top

---

Annotations Requirement 9

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
9.1.1	Documentation Review & Personnel Interview	Security policies and operational procedures related to Requirement 9	1. Can you provide the relevant documentation that outlines your security policies

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			and procedures as they pertain to Requirement 9? 2. How are these policies and procedures managed and maintained over time? 3. How are personnel informed about these policies and procedures?
9.1.2.a	Documentation Review	Descriptions of roles and responsibilities regarding activities in Requirement 9	1. Can you show me where the roles and responsibilities for Requirement 9 activities are documented? 2. How are these roles and responsibilities communicated to relevant personnel? 3. Can you provide evidence that these roles and responsibilities are regularly reviewed and updated if necessary?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
9.1.2.b	Personnel Interview	Confirmation from personnel about their understanding of their roles and responsibilities as documented	1. Can you explain your role and responsibilities regarding Requirement 9? 2. How were you informed about your roles and responsibilities? 3. Can you demonstrate or provide examples of how you fulfill your roles and responsibilities as described?
9.2.1	Observation & Personnel Interview	Records of physical security controls in place to restrict access to systems in the CDE.	1. Can you demonstrate the physical security controls in place that restrict access to systems in the CDE? 2. How are these controls monitored and maintained?
9.2.1.1.a	Location Observation	Evidence of video cameras and/or physical access control mechanisms monitoring the entry and exit points of sensitive areas within the CDE.	1. Can you show the functioning of video cameras or access control mechanisms at the entry and exit points?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			2. How do these mechanisms ensure the security of sensitive areas within the CDE?
9.2.1.1.b	Location Observation	Evidence that the video cameras or physical access control mechanisms are protected against tampering or disabling.	1. How are the video cameras or access control mechanisms protected from tampering or disabling? 2. Can you provide instances where these protections were tested or validated?
9.2.1.1.c	Observation & Personnel Interview	Documentation evidencing the review and correlation of collected data, and proof of data storage for at least three months.	1. How is data from video cameras or access control mechanisms reviewed and correlated with other entries? 2. Can you provide evidence of data storage for at least three months?
9.2.2	Observation & Personnel Interview	Records showing the controls in place to restrict access to publicly	1. Can you demonstrate the physical and/or logical controls

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		accessible network jacks within the facility.	restricting access to publicly accessible network jacks within the facility? 2. How are these controls monitored?
9.2.3	Observation & Personnel Interview	Documentation showing restricted physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility.	1. Can you show the controls in place that restrict physical access to wireless access points and other related hardware within the facility? 2. How is restricted access ensured and monitored?
9.2.4	Observation	Evidence of consoles in sensitive areas being "locked" to prevent unauthorized use.	1. Can you demonstrate a system administrator's attempt to log into "locked" consoles in sensitive areas? 2. How are these "locks" maintained and updated to prevent unauthorized access?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
9.3.1.a	Document Examination	Documented procedures detailing the authorization and management of physical access to the CDE.	1. Can you provide the documented procedures that govern physical access to the CDE? 2. How do these procedures ensure compliance with the specified elements in this requirement?
9.3.1.b	Observation & Process Verification	Identification methods such as ID badges utilized within the CDE.	1. Can you demonstrate how personnel are clearly identified within the CDE? 2. How are these identification methods managed and updated?
9.3.1.c	Process Observation	Processes showcasing that access to the identification system is limited to authorized personnel.	1. Can you illustrate how the badge system restricts access to authorized personnel only? 2. How is unauthorized access prevented in the identification process?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
9.3.1.1.a	Observation, Interview & Document Examination	Evidence of authorized access to sensitive areas and justification based on job functions.	1. Can you demonstrate how access to sensitive areas is regulated? 2. How is individual's job function determined to grant access to these areas?
9.3.1.1.b	Process Observation & Personnel Interview	Processes ensuring immediate revocation of access upon termination of personnel.	1. Can you demonstrate the process for immediate access revocation upon personnel termination? 2. What measures are in place to enforce this?
9.3.1.1.c	Document Examination & Interview	Evidence of return or disabling of physical access mechanisms for terminated personnel.	1. Can you confirm the deactivation or retrieval of access mechanisms for terminated personnel? 2. How is compliance with this requirement ensured?
9.3.2.a	Document Examination & Personnel Interview	Documented procedures for authorizing and	1. Can you present the procedures

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		managing visitor access to the CDE.	governing visitor access to the CDE? 2. How do these procedures ensure visitor access is managed as per the specified elements?
9.3.2.b	Observation & Interview	Processes demonstrating authorization and escort of visitors within the CDE.	1. Can you demonstrate the authorization process for visitors entering the CDE? 2. How is escorting of visitors within the CDE ensured?
9.3.2.c	Observation	Usage of visitor badges or other identification that prevent unescorted access to the CDE.	1. Can you show the features of visitor badges that prevent unescorted access to the CDE? 2. How is unescorted access prevented using these identifications?
9.3.2.d	Observation	Observation of visitor badge utilization and distinct identification of visitors from personnel.	1. Can you demonstrate how visitor badges distinguish

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			visitors from personnel? 2. Are all visitors required to use badges or other forms of identification?
9.3.2.e	Examination & Observation	Evidence of expiration feature on visitor badges or other identifications.	1. Can you show how visitor badges or identifications expire after a certain time? 2. How is this expiration feature managed and enforced?
9.3.3	Observation & Interview	Processes for the surrender or deactivation of visitor badges upon departure or expiration.	1. Can you illustrate the process for surrendering or deactivating visitor badges upon departure or expiration? 2. How is compliance with this procedure ensured?
9.3.4.a	Document Examination & Interview	A visitor log documenting physical access to the facility and sensitive areas.	1. Can you present the visitor log used to record physical access? 2. How is the log maintained and secured?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
9.3.4.b	Document Examination	Visitor log containing necessary details of the visit.	1. Can you confirm that the visitor log contains all the required details about the visitor and the visit? 2. How is the data in the log verified for accuracy?
9.3.4.c	Document Examination & Interview	Storage locations for visitor logs and evidence of log retention for at least three months.	1. Can you indicate where the visitor log is stored and demonstrate its secure storage? 2. How is a minimum of three months retention ensured, and what provisions are there for legal restrictions?
9.4.1	Examine documentation	Procedures for physically securing all media	1. Can you show me the documented procedures for protecting cardholder data by securing media?
9.4.1.1.a	Examine documentation	Procedures for securing offline media backups	1. How are offline media backups physically

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			secured in a secure location?
9.4.1.1.b	Interview responsible personnel and examine logs or other documentation	Secure location details and logs for offline media backups	1. Can you verify that the offline media backups are stored securely?
9.4.1.2.a	Examine documentation	Procedures for annual security review of offline media backup locations	1. Are there procedures for annually reviewing the security of offline media backup locations?
9.4.1.2.b	Interview responsible personnel and examine documented procedures, logs, or other documentation	Records of annual reviews of the security of offline media backup locations	1. Has the security of the storage location been reviewed in the last 12 months?
9.4.2.a	Examine documentation	Procedures for classifying media with cardholder data	1. Can you show me the procedures for classifying media according to data sensitivity?
9.4.2.b	Examine media logs or other documentation	Media classification logs in accordance with data sensitivity	1. Are all media classified according to the sensitivity of the data contained?
9.4.3.a	Examine documentation	Procedures for securing media sent outside the facility	1. How are the procedures defined for securing media

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			sent outside the facility?
9.4.3.b	Interview personnel and examine records	Logs and records of secured courier or other tracked delivery methods	1. Can you verify that all media sent outside the facility is logged and sent via a secure method?
9.4.3.c	Examine offsite tracking logs	Documentation of tracking details for media sent outside the facility	1. Can I see the tracking logs for all media sent outside the facility?
9.4.4.a	Examine documentation	Procedures for management approval for media moved outside the facility	1. What are the procedures for management approval for media transport outside the facility?
9.4.4.b	Interview responsible personnel and examine offsite media tracking logs	Management authorization records and offsite media tracking logs	1. Can you demonstrate that management authorization was obtained for media moved outside?
9.4.5.a	Examine documentation	Procedures for maintaining electronic media inventory logs	1. Can you show me the procedures for maintaining electronic media inventory logs?
9.4.5.b	Interview responsible personnel and examine	Maintained electronic media inventory logs	1. Are electronic media inventory

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
	electronic media inventory logs		logs maintained regularly?
9.4.5.1.a	Examine documentation	Procedures for annual electronic media inventories	1. Can you show me the procedures for conducting annual electronic media inventories?
9.4.5.1.b	Interview personnel and examine electronic media inventory logs	Records of annual electronic media inventories	1. Can you verify that media inventories are conducted at least annually?
9.4.6.a	Examine the periodic media destruction policy	Procedures for destroying hard-copy media	1. What are the procedures for destroying hard-copy media when it's no longer needed?
9.4.6.b	Observe processes and interview personnel	Evidence of hard-copy media destruction methods	1. How is hard-copy media destroyed to prevent data reconstruction?
9.4.6.c	Observe storage containers	Secure containers for storing materials to be destroyed	1 Can you show me the secure containers used for storing materials awaiting destruction?
9.4.7.a	Examine the periodic media destruction policy	Procedures for destroying electronic media	1. Can you detail the procedures for destroying electronic media

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			when it's no longer needed?
9.4.7.b	Observe the media destruction process and interview responsible personnel	Evidence of compliant electronic media destruction methods	1. How is electronic media destroyed to ensure cardholder data cannot be reconstructed?
9.5.1	Document Examination	Documented policies and procedures detailing processes for handling POI devices	1. Can you provide the policies and procedures that detail the processes implemented to adhere to requirement 9.5.1?
9.5.1.1.a	Document Examination	List of POI devices containing all elements specified in this requirement	1. Can you provide the latest list of POI devices and demonstrate that it includes all the necessary elements as specified in this sub-requirement?
9.5.1.1.b	Observation & Document Comparison	An accurate and up-to-date list of POI devices and device locations	1. Can you demonstrate that the POI device list is accurate and up-to-date by comparing it with the actual devices

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			and their locations?
9.5.1.1.c	Interview	Evidence of regular updates to the list of POI devices (e.g., change logs, version history)	1. Can you explain the process followed to update the list of POI devices when devices are added, relocated, or decommissioned?
9.5.1.2.a	Document Examination	Documented procedures for periodic inspections of POI devices	1. Can you provide the documented procedures that detail the periodic inspection process of POI device surfaces to detect tampering and unauthorized substitution?
9.5.1.2.b	Interview & Observation	Training materials, employee testimonies about awareness of inspection procedures	1. Can you demonstrate that personnel are aware of and adhere to the procedures for inspecting devices, and are the inspections conducted periodically?
9.5.1.2.1.a	Document Examination	Targeted risk analysis for the frequency of periodic	1. Can you provide the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		POI device inspections	targeted risk analysis documentation that defines the frequency and type of inspections performed for POI devices?
9.5.1.2.1.b	Interview & Document Examination	Documented results of periodic device inspections and interview records	1. Can you verify that the frequency and type of POI device inspections performed are in line with what is defined in the risk analysis conducted for this requirement?
9.5.1.3.a	Document Examination	Training materials for personnel in POI environments	1. Can you provide the training materials prepared for personnel in POI environments that cover all elements specified in this sub-requirement?
9.5.1.3.b	Interview	Training records, personnel testimony regarding training received	1. Can you verify that personnel in POI environments have received adequate training and are knowledgeable

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			about the procedures as specified in this sub-requirement?

annotations 9 | annotations | requirements | principles | top

Annotations Requirement 10

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
10.1.1	Document Examination and Personnel Interview	Security policies and operational procedures documentation related to Requirement 10.	1. Can you provide the security policies and operational procedures for Requirement 10? 2. How are these policies managed and maintained in line with the stipulations of Requirement 10?
10.1.2.a	Document Examination	Documentation detailing the descriptions of roles and responsibilities for activities under Requirement 10.	1. Can you show where the roles and responsibilities for activities under Requirement 10 are documented? 2. Are these roles clearly assigned to specific personnel or teams?
10.1.2.b	Personnel Interview	Direct communication with personnel	1. Can you describe your role and responsibilities as

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		responsible for activities under Requirement 10.	they pertain to Requirement 10? 2. How were these responsibilities communicated to you?
10.2.1	System Administrator Interview and Document Examination	System configurations and evidence of active audit logs for all system components.	1. Can you demonstrate that audit logs are enabled and active for all system components?
10.2.1.1	Document Examination	Audit log configurations and log data indicating individual user access to cardholder data.	1. Can you show where individual user access to cardholder data is logged within the audit configurations?
10.2.1.2	Document Examination	Audit log configurations and log data capturing actions by individuals with administrative access.	1. Are all actions undertaken by individuals with administrative access logged?
10.2.1.3	Document Examination	Audit log configurations and log data detailing access to all audit logs.	1. How is access to all audit logs captured in the system?
10.2.1.4	Document Examination	Audit log configurations and log data indicating invalid logical access attempts.	1. How does the system capture and log invalid logical access attempts?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
10.2.1.5	Document Examination	Log data and configurations documenting changes to identification and authentication credentials.	1. Can you demonstrate how changes to identification and authentication credentials are logged?
10.2.1.6	Document Examination	Audit log configurations and log data complying with all elements specified in this requirement.	1. How does the audit log configuration adhere to the stipulations mentioned in this requirement?
10.2.1.7	Document Examination	Audit log configurations and log data capturing creation and deletion of system level objects.	1. Can you verify that log data captures the creation and deletion of system-level objects?
10.2.2	Personnel Interview and Document Examination	Audit log configurations and log data showing inclusion of all elements specified in this requirement in log entries for each auditable event.	1. Can you demonstrate that all specified elements are included in log entries for each auditable event from 10.2.1.1 through 10.2.1.7?
10.3.1	System Administrators Interview and Document Examination	System configurations, privileges documentation, and details of individuals granted read access to audit log files	1. Can you provide a list of individuals with read access to audit log files and justify their job-related needs for this access?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		based on job necessity.	
10.3.2	Document Examination and System Administrators Interview	System configurations, privileges documentation, and strategies implemented to protect current audit log files from unauthorized modifications.	1. Can you demonstrate the measures in place to protect current audit log files from unauthorized modifications, including access control mechanisms, physical or network segregation?
10.3.3	Document Examination	Backup configurations or log files detailing the backup strategy for current audit log files, including methods to secure central internal log servers or other media.	1. Can you show the backup configurations that ensure current audit log files are promptly backed up to a secure and central internal log server or other unmodifiable media?
10.3.4	Document Examination	Documentation of system settings, monitored files, and results from monitoring activities that verify the implementation of file integrity monitoring or change-detection software on audit logs.	1. How is file integrity monitoring or change-detection software utilized for monitoring audit logs? 2. Can you provide recent results from these monitoring activities?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
10.4.1.a	Document Examination	Security policies and procedures documenting the daily review of all elements specified in the requirement.	1. Can you provide the policy that outlines the daily review process for all elements specified in this requirement?
10.4.1.b	Process Observation and Personnel Interview	Evidence of daily review processes and interviews with personnel involved in the daily review of specified elements.	1. Can you demonstrate the daily review process in action, and explain how all elements specified in the requirement are reviewed daily?
10.4.1.1	Document Examination and Personnel Interview	Log review mechanisms documentation and interviews confirming the use of automated mechanisms for log reviews.	1. Can you describe and demonstrate how automated mechanisms are utilized for daily log reviews?
10.4.2.a	Document Examination	Security policies and procedures detailing the periodic review of logs for all other system components.	1. Can you provide the policy that details the periodic review process for logs of all other system components?
10.4.2.b	Document Examination and Personnel Interview	Documented results of log reviews and interviews confirming the periodic execution of log reviews.	1. Can you show the documented results of recent periodic log reviews, and explain the process

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			undertaken for these reviews?
10.4.2.1.a	Document Examination	Documentation of targeted risk analysis for the frequency of periodic log reviews concerning elements in Requirement 12.3.1.	1. Can you show the targeted risk analysis for determining the frequency of periodic log reviews in line with Requirement 12.3.1?
10.4.2.1.b	Document Examination and Personnel Interview	Documented results of periodic log reviews as per the risk analysis, and interviews with personnel to confirm the adherence to the stipulated frequency.	1. Can you present documented results of periodic log reviews as per the risk analysis, and discuss the frequency and findings?
10.4.3.a	Document Examination	Security policies and procedures documenting the process for addressing exceptions and anomalies identified during the review process.	1. Can you provide the policies and procedures that detail how exceptions and anomalies identified during log reviews are addressed?
10.4.3.b	Process Observation and Personnel Interview	Observations and interviews with personnel to verify the active addressing of identified exceptions and anomalies.	1. Can you demonstrate the process followed when exceptions and anomalies are identified during log reviews, and

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			discuss recent examples?
10.5.1.a	Document Examination	- Audit log retention policies documentation. - Procedures documentation for retaining audit log history for at least 12 months, with a minimum of the recent three months being readily available online.	1. Could you please provide the documentation defining your audit log retention policies? 2. Can you showcase the procedural document detailing the retention of audit log history for at least 12 months, with at least the most recent three months available online?
10.5.1.b	Document Examination, Personnel Interview, and Audit Log Examination	- Configurations settings showcasing the audit log history retention. - Interviews with personnel responsible for managing audit logs. 2. Audit logs evidencing retention for at least 12 months.	1. Can you guide me through the configurations set up to retain audit log history for at least 12 months? 2. Can you explain how the process of retaining audit log history is maintained and managed? 3. Could you please show the actual audit logs demonstrating a history of at least 12 months?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
10.5.1.c	Personnel Interview and Process Observation	- Interviews with personnel confirming the availability of the most recent three months' audit log history. - Observation of the processes ensuring the immediate availability of the most recent three months' audit log history for analysis.	1. Could you elucidate how the most recent three months of audit log history is made immediately available for analysis? 2. Can you demonstrate the process ensuring that the recent three months' audit log history is readily accessible?
10.6.1	System Configuration Settings Examination	- Evidence of the implementation and updating of time-synchronization technology.	1. Can you show how time-synchronization technology is implemented on your systems? 2. How is it kept current?
10.6.2	System Configuration Settings Examination	- Detailed configuration settings related to the acquisition, distribution, and storage of the correct time.	1. Can you show the configuration settings that ensure the acquisition, distribution, and storage of the correct time?
10.6.3.a	System Configuration and Settings Examination	- System configurations displaying restricted access to time data. - List of personnel with granted access.	1. How is access to time data restricted within the system settings? 2. Can you provide a list of personnel

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			who have access based on business needs?
10.6.3.b	System Configuration, Settings, and Logs Examination; Process Observation	- System configurations indicating logging of time setting changes on critical systems. - Logs showing monitored changes and reviews conducted.	1. Can you demonstrate how changes to time settings on critical systems are logged and monitored? 2. Can you showcase the process for reviewing these logs?
10.7.1.a	Documentation Examination (Service Provider Assessments Only)	- Documentation outlining processes for the detection and addressing of critical security control system failures, inclusive of all elements specified in the requirement.	1. Can you show the documentation that details your processes for detecting and addressing failures in critical security control systems?
10.7.1.b	Process Observation and Personnel Interview (Service Provider Assessments Only)	- Observational evidence of detection and alerting processes. - Testimonies from personnel regarding the processes and alert generation in case of control failure.	1. How are failures in critical security control systems detected and reported? 2. Can you demonstrate how a failure triggers an alert?
10.7.2.a	Documentation Examination	- Documentation defining the processes for the prompt detection and addressing of critical	1. Could you provide documentation that explains the processes in place

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		security control system failures, including all specified elements.	for the rapid detection and addressing of critical security control system failures?
10.7.2.b	Process Observation and Personnel Interview	- Evidence of detection and alerting processes in action. - Interview records demonstrating the reporting and alert mechanisms during a critical security control failure.	1. How is the detection and alerting process for critical security control system failures conducted? 2. Can you showcase a situation where a failure generated an alert?
10.7.3.a	Documentation Examination and Personnel Interview	- Documentation verifying defined and implemented processes for responding to critical security control system failures with all specified elements. - Interview records affirming the implementation of the defined processes.	1. Can you elucidate on the processes defined to respond to failures of critical security control systems? 2. How are these processes implemented in real-time situations?
10.7.3.b	Records Examination	- Records showing documentation of security control system failures including identified causes, the duration,	1. Could you showcase records where security control system failures were documented with

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		and remediation details.	necessary details? 2. How is the root cause addressed during these occurrences?

annotations 10 | annotations | requirements | principles | top

Annotations Requirement 11

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
11.1.1	Documentation review and Personnel Interview	Security policies and operational procedures documents that outline how the various elements specified in requirement 11 are managed.	1. Can you provide the security policies and operational procedures that pertain to requirement 11? 2. How are these policies and procedures managed and updated to align with requirement 11? 3. Can you showcase how these policies align with the defined approach testing procedures?
11.1.2.a	Documentation review	Formal documentation that explicitly states the roles and responsibilities for	1. Can you provide the documented roles and responsibilities for carrying out activities as per

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		activities in requirement 11.	requirement 11? 2. How are individuals assigned these roles and responsibilities? 3. Can you show where these roles and responsibilities are documented?
11.1.2.b	Personnel Interview	Evidence that personnel understand and acknowledge their assigned roles and responsibilities in line with requirement 11.	1. Can you explain your role and responsibilities in carrying out activities as per requirement 11? 2. How were you informed about your responsibilities? 3. Can you demonstrate your understanding of your role in adherence to requirement 11?
11.2.1.a	Documentation review	Policies and procedures documentation that outlines the management processes for both authorized and unauthorized wireless access points as per the requirement.	1. Can you provide the policies and procedures that detail the management of authorized and unauthorized wireless access points? 2. How do these policies ensure compliance with all

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			the elements specified in this requirement?
11.2.1.b	Documentation review and Personnel Interview	Methodology documents that explain how both authorized and unauthorized wireless access points are detected and identified, alongside interviews to confirm adherence.	1. Can you explain the methodologies in place for identifying and detecting unauthorized and authorized wireless access points? 2. How does the methodology ensure alignment with the elements specified in this requirement? 3. Can personnel demonstrate their understanding and adherence to the methodologies in place?
11.2.1.c	Documentation review and Personnel Interview	Documentation of wireless assessment results and interview notes to confirm the assessments were conducted according to the specified elements in this requirement.	1. Can you provide recent wireless assessment results? 2. How do these assessments align with the elements outlined in the requirement? 3. Can personnel explain the process followed for wireless assessments?
11.2.1.d	Configuration Review	Verification of configuration settings to ensure	1. Can you showcase the configuration

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		the automated monitoring system generates alerts to notify relevant personnel.	settings of the automated monitoring system? 2. How does the system generate alerts to notify personnel? 3. Can you demonstrate a previous instance where the alert mechanism worked as configured?
11.2.2	Documentation review	Documented inventory of authorized wireless access points, including a business justification for each.	1. Can you provide the current inventory of authorized wireless access points? 2. Is there a documented business justification for each authorized wireless access point? 3. How is the inventory maintained and updated?
11.3.1.a	Document Examination	Internal scan report results from the last 12 months	1. Can you show the internal scan reports from each of the last four quarters? 2. Can you demonstrate that scans occurred at least quarterly?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
11.3.1.b	Document Examination	Internal scan and rescan reports highlighting the resolution of high-risk and critical vulnerabilities as per Requirement 6.3.1	1. Can you showcase where high-risk and critical vulnerabilities were identified and resolved within the internal scan reports? 2. How were these vulnerabilities addressed?
11.3.1.c	Document Examination and Personnel Interview	Scan tool configurations and latest vulnerability update details	1. How do you ensure that the scan tool is up-to-date with the latest vulnerability information? 2. Can you demonstrate the current configuration of the scan tool?
11.3.1.d	Personnel Interview	Evidence of qualification and organizational independence of the personnel responsible for the scans	1. Can you confirm who performed the scans? 2. Can you verify the organizational independence of the scanner?
11.3.1.1.a	Document Examination	Entity’s risk analysis documentation as per Requirement 12.3.1	1. Can you provide the risk analysis conducted as per Requirement 12.3.1? 2. How does this analysis define the risk associated with

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			various vulnerabilities?
11.3.1.1.b	Document Examination and Personnel Interview	Internal scan reports and other documentation evidencing risk analysis adherence	1. Can you demonstrate how vulnerabilities have been addressed based on the defined risk analysis? 2. Can you show evidence of rescans confirming vulnerability resolution?
11.3.1.2.a	Document Examination	Scan tool configurations showcasing authenticated scanning parameters	1. Can you show the configuration settings that enable authenticated scanning? 2. How do you ensure that scanning credentials have sufficient privileges?
11.3.1.2.b	Document Examination and Personnel Interview	Scan report results and evidence of authenticated scanning practices	1. Can you provide reports showcasing the results of authenticated scans? 2. Can personnel explain the process and benefits of authenticated scanning?
11.3.1.2.c	Document Examination and Personnel Interview	Account details used for	1. Can you provide details on the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		authenticated scanning and adherence to Requirement 8.2.2	accounts used for authenticated scanning? 2. How are these accounts managed as per Requirement 8.2.2?
11.3.1.2.d	Document Examination	Documentation defining systems unable to accept credentials for authenticated scanning	1. Can you list the systems that are unable to accept credentials for authenticated scanning? 2. How is this information documented and managed?
11.3.1.3.a	Document Examination	Change control documentation and internal scan reports post significant changes	1. Can you provide documentation on significant changes and subsequent scans? 2. How do scan reports reflect these changes?
11.3.1.3.b	Document Examination and Personnel Interview	Internal scan and rescan reports highlighting actions post significant changes	1. Can you provide evidence of scans performed after significant changes? 2. How were high-risk and critical vulnerabilities addressed?
11.3.1.3.c	Personnel Interview	Evidence of qualification and	1. Can you confirm the qualifications of

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		organizational independence of the personnel conducting scans	personnel performing internal scans? 2. How do you ensure organizational independence of the scanner?
11.3.2.a	Document Examination	Approved Scanning Vendor (ASV) reports from the last 12 months	1. Can you provide the ASV scan reports from each of the last four quarters? 2. Can you demonstrate quarterly external vulnerability scans?
11.3.2.b	Document Examination	ASV scan and rescan reports showcasing vulnerability resolution and adherence to ASV Program Guide requirements	1. Can you demonstrate the resolution of vulnerabilities as per ASV Program Guide requirements? 2. Can you show evidence of passing scan results?
11.3.2.c	Document Examination	ASV scan reports indicating completion by a PCI SSC Approved Scanning Vendor	1. Can you confirm the ASV scan reports were completed by a PCI SSC Approved Scanning Vendor? 2. Can you provide credentials of the ASV?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
11.3.2.1.a	Document Examination	Change control documentation and external scan reports post significant changes	1. Can you provide documentation showcasing scans post significant changes? 2. How do external scan reports reflect these changes?
11.3.2.1.b	Document Examination and Personnel Interview	External scan and rescan reports with evidence of vulnerability resolution as per CVSS scoring	1. Can you demonstrate resolution of vulnerabilities scored 4.0 or higher by the CVSS within the scan reports? 2. Can personnel explain the process followed to resolve these vulnerabilities?
11.3.2.1.c	Personnel Interview	Evidence of qualification and organizational independence of the personnel or third party conducting external scans	1. Can you confirm the qualifications of the personnel or third party performing external scans? 2. How do you ensure organizational independence of the tester?
11.4.1	Documentation Review, Personnel Interview	Penetration testing methodology documentation.	1. Can you provide the documented penetration testing methodology that includes all the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			elements specified in this requirement?
11.4.2.a	Documentation Review, Scope of Work Review	Scope of work and results from the most recent internal penetration test.	1. Can you show how the internal penetration test was conducted in accordance with the elements specified in this requirement?
11.4.2.b	Personnel Interview	Evidence of tester qualifications and organizational independence.	1. Can you verify that the internal penetration test was conducted by a qualified resource with organizational independence?
11.4.3.a	Documentation Review, Scope of Work Review	Scope of work and results from the most recent external penetration test.	1. Can you show how the external penetration test was conducted according to the elements specified in this requirement?
11.4.3.b	Personnel Interview	Evidence of tester qualifications and organizational independence.	1. Can you verify that the external penetration test was conducted by a qualified resource with organizational independence?
11.4.4	Documentation Review	Penetration testing results and evidence of corrections made for exploitable vulnerabilities.	1. Can you show the actions taken to correct exploitable vulnerabilities and security weaknesses

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			identified in the penetration tests?
11.4.5.a	Documentation Review, Segmentation Control Review	Segmentation controls documentation and penetration testing methodology covering segmentation methods.	1. Can you verify that the penetration testing procedures are defined to test all segmentation methods as specified in this requirement?
11.4.5.b	Documentation Review, Penetration Test Review	Results from the most recent penetration test covering all specified elements.	1. Can you show that the most recent penetration test covers and addresses all elements specified in this requirement?
11.4.5.c	Personnel Interview	Evidence of tester qualifications and organizational independence.	1. Can you verify that the test was performed by a qualified resource with organizational independence?
11.4.6.a	Documentation Review (Service Provider Assessments Only)	Results from the most recent penetration test covering all specified elements.	1. Can you demonstrate that the most recent penetration test covers and addresses all elements specified in this requirement?
11.4.6.b	Personnel Interview (Service Provider Assessments Only)	Evidence of tester qualifications and organizational independence.	1. Can you confirm that the test was performed by a qualified resource

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			with organizational independence?
11.4.7	Documentation Review (Multi-Tenant Service Provider Assessments Only)	Evidence supporting external penetration testing per Requirements 11.4.3 and 11.4.4 for customers.	1. Can you provide evidence that supports your customers for external penetration testing as specified in Requirements 11.4.3 and 11.4.4?
11.5.1.a	Documentation Review, Network Diagram Analysis	System configurations, network diagrams	1. Can you show where the intrusion-detection and/or intrusion-prevention techniques are implemented at the perimeter and critical points in the CDE?
11.5.1.b	Documentation Review, Personnel Interview	System configurations, testimonials from responsible personnel	1. Can you demonstrate how the intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises?
11.5.1.c	Documentation Review	System configurations, vendor documentation	1. How do you ensure that all engines, baselines, and signatures related to intrusion-detection and/or intrusion-prevention

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			techniques are kept up to date?
11.5.1.1.a (Service Provider Assessments Only)	Documentation Review, Configuration Settings Analysis	Documentation, configuration settings	1. Can you prove that methods to detect and alert on/prevent covert malware communication channels are operational?
11.5.1.1.b (Service Provider Assessments Only)	Documentation Review	Incident-response plan (Requirement 12.10.1)	1. How does your incident-response plan address the detection of covert malware communication channels?
11.5.1.1.c (Service Provider Assessments Only)	Personnel Interview, Process Observation	Testimonials from responsible personnel, process documentation	1. Can you explain how your personnel maintain knowledge of covert malware communication and control techniques and the procedure for responding to suspected malware?
11.5.2.a	Documentation Review, System Settings Analysis	System settings, monitored files, monitoring activity results	1. Can you demonstrate the functionality of your change-detection mechanism and how it is used?
11.5.2.b	Configuration Review	Change-detection mechanism settings	1. How is the change-detection mechanism

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			configured to comply with the elements specified in this requirement?
11.6.1.a	Documentation Review, System Settings Analysis	System settings, monitored payment pages, monitoring activity results	1. Can you demonstrate how the change- and tamper-detection mechanism operates and how it monitors payment pages?
11.6.1.b	Configuration Review	Configuration settings for the change- and tamper-detection mechanism	1. Can you show how the change- and tamper-detection mechanism is configured in accordance with all the elements specified in this requirement?
11.6.1.c	Risk Analysis Review	Documentation on targeted risk analysis performed in line with Requirement 12.3.1	1. Can you explain the risk analysis process that determined the frequency of the change- and tamper-detection mechanism's functions and show that it aligns with Requirement 12.3.1?
11.6.1.d	Configuration Review, Personnel Interview	Configuration settings, interviews	1. How often does the change- and

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		with personnel responsible for the mechanism, documentation on targeted risk analysis	tamper-detection mechanism function and how does this frequency align with either the once every seven days standard or the entity's targeted risk analysis?

annotations 11 | annotations | requirements | principles | top

Annotations Requirement 12

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
12.1.1	Document Examination & Personnel Interview	1. Information security policy document 2. Records of policy updates and management practices	1. Can you demonstrate how the information security policy is managed and updated in line with the PCI DSS requirements? 2. How are personnel informed about the updates in the information security policy?
12.1.2	Document Examination & Responsible Personnel Interview	1. Information security policy document 2. Records of policy management procedures	1. Can you explain the management process for the information security policy? 2. How do you ensure that all elements specified in

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			this requirement are included and managed within the policy?
12.1.3.a	Document Examination	1. Information security policy document 2. Document outlining defined roles and responsibilities related to information security	1. Can you show where the information security roles and responsibilities are clearly defined for all personnel within the policy documents? 2. How are these roles communicated to the respective personnel?
12.1.3.b	Personnel Interview in Various Roles	1. Training records 2. Documentation outlining information security responsibilities per role	1. Can you describe your information security responsibilities as per your role? 2. How were you informed or trained about these responsibilities?
12.1.3.c	Document Examination	1. Signed acknowledgments from personnel regarding their information security responsibilities	1. Can you provide documentation showing that personnel acknowledge their information security responsibilities? 2. What process is in place to ensure that all personnel

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			acknowledge their responsibilities?
12.1.4	Document Examination	1. Information security policy document 2. Official documentation assigning a CISO or equivalent role	1. Can you show where the responsibility for information security is formally assigned within the organization? 2. How does the assigned executive manage and oversee information security in the organization?
12.2.1	Document Examination & Responsible Personnel Interview	1. Acceptable use policies for end-user technologies 2. Documentation evidencing the implementation of said policies	1. Can you provide the acceptable use policy pertaining to end-user technologies? 2. How are these policies communicated to and acknowledged by the personnel? 3. Can you demonstrate the implementation of the processes as documented in the policy?
12.3.1	Document Examination	1. Documented policies and procedures outlining the process for targeted risk analyses 2. Evidence of	1. Can you provide the policies and procedures for targeted risk analyses related to each PCI DSS

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		adherence to the process including frequency and inclusivity of all elements as per this requirement	requirement? 2. How do these policies ensure flexibility in the frequency of analyses conducted? 3. Can you demonstrate the inclusion of all elements specified in this requirement within the process?
12.3.2	Document Examination	1. Documented targeted risk analyses for each PCI DSS requirement 2. Evidence that the documentation is in line with all elements specified in this requirement	1. Can you showcase the documentation for targeted risk analyses pertaining to each PCI DSS requirement? 2. How do you ensure that the analyses align with all elements specified in this requirement?
12.3.3	Document Examination & Personnel Interview	1. Documentation detailing the cryptographic suites and protocols in use 2. Records of reviews conducted on the aforementioned documentation	1. Can you provide the documentation which outlines the cryptographic suites and protocols currently in use? 2. Can you demonstrate that the documentation and reviews are in accordance with all

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
			the elements specified in this requirement? 3. How do you approach the review process for cryptographic suites and protocols?
12.3.4	Document Examination & Personnel Interview	1. Documentation detailing the review of hardware and software technologies in use 2. Records of personnel interviews and reviews conducted in line with this requirement	1. Could you provide the documentation of the reviews conducted on hardware and software technologies currently in use? 2. Can personnel elucidate the process followed for the reviews? 3. How do you ensure that the reviews are conducted in accordance with all elements specified in this requirement?
12.4.1	Document Examination	1. Documented proof of executive management establishing responsibility for cardholder data protection 2. Evidence of a PCI DSS compliance	1. Can you provide documentation where executive management has assigned responsibilities for cardholder data protection? 2. How does the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		program incorporating all elements specified in this requirement	established PCI DSS compliance program incorporate all the elements specified in this requirement?
12.4.2.a	Document Examination	1. Policies and procedures detailing the process for conducting reviews of personnel tasks 2. Evidence that the processes are in line with all security policies and operational procedures, including those specified in this requirement	1. Can you provide the policies and procedures that detail how reviews are conducted to confirm personnel adherence to security policies and operational procedures? 2. How do these procedures ensure compliance with all the tasks specified in this requirement?
12.4.2.b	Document Examination	1. Policies and procedures detailing the process for conducting reviews of personnel tasks 2. Evidence that the processes are in line with all security policies and operational procedures, including those specified in this requirement	1. Can you provide the policies and procedures that detail how reviews are conducted to confirm personnel adherence to security policies and operational procedures? 2. How do these procedures ensure compliance with all the tasks specified in this requirement?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
12.4.2.1	Document Examination	1. Documentation from reviews conducted per PCI DSS Requirement 12.4.2 2. Evidence that the documentation encompasses all elements specified in this requirement	1. Can you showcase the documentation derived from reviews conducted as per PCI DSS Requirement 12.4.2? 2. How does the documentation comply with all elements specified in this requirement?
12.5.1.a	Document Examination	1. Inventory list of all in-scope system components 2. Descriptions of function/use for each listed component	1. Can you provide the inventory list that includes all in-scope system components? 2. How does the inventory detail the function/use of each component?
12.5.1.b	Personnel Interview	Evidence that the inventory list is maintained and updated regularly	1. How do you ensure that the inventory list is kept current?
12.5.2.a	Document Examination and Personnel Interview	1. Documented results of scope reviews 2. Evidence of regular reviews at least annually and post significant changes to the in-scope environment	1. Can you demonstrate the frequency of the scope reviews? 2. How are scope reviews conducted following significant changes to the in-scope environment?
12.5.2.b	Document Examination	Documentation that confirms PCI DSS	1. Can you provide documented results

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		scoping activities include all elements specified in this requirement	of PCI DSS scoping confirmation activities that adhere to the criteria specified in this requirement?
12.5.2.1.a	Document Examination and Personnel Interview	1. Documented results of scope reviews conducted at least semi-annually 2. Evidence of reviews following significant changes	1. Can you provide documentation of semi-annual scope reviews? 2. How are reviews handled following significant changes?
12.5.2.1.b	Document Examination	Documentation that confirms scoping validation includes all elements specified in Requirement 12.5.2	1. Can you provide evidence that scoping validation activities encompass all elements mentioned in Requirement 12.5.2?
12.5.3.a	Document Examination	1. Policies and procedures outlining the review process for significant organizational structure changes 2. Evidence of review impacting PCI DSS scope and controls	1. Can you showcase policies and procedures that dictate the review process following substantial changes to the organizational structure?
12.5.3.b	Document Examination and Personnel Interview	1. Documentation of reviews (e.g., meeting minutes) 2. Evidence of communication of review results to	1. Can you provide documentation of reviews triggered by substantial changes to the organizational structure?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		executive management	2. How were these results communicated to executive management?
12.6.1	Document Examination	Security awareness program documentation detailing the entity's information security policy and procedures, and personnel's roles regarding cardholder data protection.	1. Can you provide documentation that illustrates how the security awareness program informs personnel about the security policy and their roles in protecting cardholder data?
12.6.2	Document Examination and Personnel Interview	1. Content of the security awareness program 2. Evidence of content reviews	1. Can you demonstrate the content and structure of the security awareness program? 2. How are reviews of the program conducted and documented?
12.6.3.a	Document Examination	Records demonstrating that personnel attend security awareness training upon hire and at least annually.	1. Can you provide records showcasing that personnel undergo security awareness training upon hire and at least once every 12 months?
12.6.3.b	Document Examination	Materials showcasing the various methods used within the	2. What different methods are employed in the

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		security awareness program to communicate awareness and educate personnel.	security awareness program to communicate awareness and educate personnel?
12.6.3.c	Personnel Interview	Evidence from personnel interviews indicating completion of awareness training and understanding of their role in protecting cardholder data.	1. Can you confirm that personnel have completed awareness training and are aware of their responsibilities in protecting cardholder data?
12.6.3.d	Document Examination	Acknowledgments from personnel, dated at least once every 12 months, confirming that they have read and understand the information security policy and procedures.	1. Can you present personnel acknowledgments indicating they have read and understood the information security policy and procedures at least annually?
12.6.3.1	Document Examination	Documentation detailing the content of the security awareness training, ensuring it encompasses all elements specified in this requirement.	Does the security awareness training content include all elements specified in this sub-requirement?
12.6.3.2	Document Examination	Security awareness training materials showcasing content on the acceptable	1. Can you demonstrate that the security awareness training content

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		use of end-user technologies as stipulated in Requirement 12.2.1.	incorporates awareness regarding the acceptable use of end-user technologies per Requirement 12.2.1?
12.7.1	Interview with HR Department Management	1. HR policies related to personnel screening before hiring 2. Records of screening processes performed for personnel who have access to the Cardholder Data Environment (CDE).	1. Can you describe the screening process conducted for potential hires who will have access to the CDE? 2. How do you ensure compliance with local laws during the screening process? 3. Can you provide records of screening processes conducted for recently hired personnel who have access to the CDE?
12.8.1.a	Document Examination	Policies and procedures describing the maintenance of a list of TPSPs and the services they provide.	1. How are the processes defined to maintain a list of TPSPs and the services they provide
12.8.1.b	Document Examination	A maintained list of all TPSPs with a description of the services provided.	1. Can you provide the current list of TPSPs along with a description of services each one provides?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
12.8.2.a	Document Examination	Policies and procedures documenting the requirement of maintaining written agreements with all TPSPs in line with the specifics of this requirement.	1. How are the processes defined to maintain written agreements with TPSPs in line with this requirement
12.8.2.b	Document Examination	Copies of written agreements with TPSPs maintained as per the elements specified in this requirement.	1. Can you provide copies of the written agreements with TPSPs which align with the specifications of this requirement?
12.8.3.a	Document Examination	Policies and procedures outlining the due diligence processes for engaging TPSPs.	2. What processes are defined for conducting due diligence before engaging with TPSPs
12.8.3.b	Document Examination & Personnel Interview	Evidence of due diligence undertaken prior to engaging TPSPs.	1. Can you provide evidence of due diligence conducted prior to engaging with TPSPs
12.8.4.a	Document Examination	Policies and procedures detailing the monitoring of TPSPs' PCI DSS compliance status annually.	2. What processes are defined for monitoring the PCI DSS compliance status of TPSPs annually
12.8.4.b	Document Examination & Personnel Interview	Documentation evidencing the annual	1. Can you provide documentation

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		monitoring of each TPSP's PCI DSS compliance status.	showing the annual monitoring of TPSPs' PCI DSS compliance status
12.8.5.a	Document Examination	Policies and procedures documenting the information maintenance regarding PCI DSS requirements managed by each TPSP and the entity.	1. How are the processes defined to maintain information about PCI DSS requirements managed by each TPSP and the entity
12.8.5.b	Document Examination & Personnel Interview	Documentation showcasing the information about PCI DSS requirements managed by each TPSP and the entity, and any shared responsibilities.	1. Can you provide documentation detailing the PCI DSS requirements managed by each TPSP, the entity, and any shared responsibilities
12.9.1	Document Examination	TPSP policies, procedures, and templates used for drafting written agreements including written acknowledgments in line with the specifics of this requirement.	1. Can you provide the policies, procedures, and templates used for crafting written agreements, especially focusing on written acknowledgments as stipulated in this requirement?
12.9.2	Document Examination	Policies and procedures that detail the processes TPSPs	1. Can you show the policies and procedures that

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		use to support customers' requests for information as per Requirements 12.8.4 and 12.8.5.	outline how TPSPs address customers' information requests in line with Requirements 12.8.4 and 12.8.5?
12.10.1.a	Document Examination	Incident response plan documentation, detailing the elements specified in this requirement.	1. Could you provide the incident response plan and illustrate how it encompasses the elements mentioned in the requirement?
12.10.1.b	Interview & Document Examination	Documentation and records from previously reported incidents or alerts.	1. Can you demonstrate with past incident documentation that the incident response plan and procedures were adhered to during previous incidents or alerts?
12.10.2	Interview & Document Review	Documentation evidencing the annual review and testing of the incident response plan, including modifications made based on the testing and elements listed in Requirement 12.10.1.	1. How is the annual review and testing of the security incident response plan conducted, and can you show documentation to verify the inclusion of elements mentioned in Requirement 12.10.1?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
12.10.3	Interview & Document Examination	Documentation specifying personnel assigned for 24/7 availability in case of security incidents.	1. Could you identify the personnel designated to be on-call 24/7 for security incidents and how their roles are defined in the documentation?
12.10.4	Interview & Training Documentation Review	Training documentation highlighting the periodic training schedule and content for incident response personnel.	1. Can you provide evidence of the periodic training undergone by incident response personnel and describe their responsibilities as outlined in the training documentation?
12.10.4.1.a	Document Examination	Documentation detailing the entity's targeted risk analysis pertaining to the frequency of training for incident response personnel, complying with the guidelines specified in Requirement 12.3.1.	1. Could you showcase the risk analysis conducted to determine the training frequency for incident response personnel, ensuring it aligns with the elements stated in Requirement 12.3.1?
12.10.4.1.b	Interview & Document Examination	Records of periodic training results and interviews confirming the adherence to the frequency defined through risk analysis	1. Can you demonstrate through records and personnel interviews that the training is conducted as frequently as defined

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
		as per this requirement.	through the entity's risk analysis for this requirement?
12.10.5	Document Examination & Observation	Documentation and practical demonstrations of how monitoring and responding to alerts from security monitoring systems are incorporated into the security incident response plan.	1. Could you detail how the incident response processes encompass monitoring and responding to alerts from security monitoring systems, also demonstrating it practically?
12.10.6.a	Document Examination	Policies and procedures illustrating the defined processes for evolving the security incident response plan based on lessons learned and industry developments.	1. Could you provide the policies and procedures that detail the processes for adapting the incident response plan based on lessons learned and industry trends?
12.10.6.b	Interview & Document Examination	Documentation of the evolved security incident response plan along with interviews of responsible personnel elucidating on how the plan is modified to incorporate lessons learned and industry advancements.	1. Can you demonstrate through documentation and interviews how the incident response plan has evolved over time, including adaptations based on lessons learned and industry developments?

Sub-Requirement	Type of Interview/Observation	Documentation & Evidence Expected	QSA Questions
12.10.7.a	Document Examination	Documented incident response procedures highlighting the steps to be taken upon detection of unexpected stored PAN, including all the elements specified in this requirement.	1. Could you present the documented procedures outlining the steps to be taken in the event of detecting unexpected stored PAN, ensuring that it encompasses all elements outlined in this requirement?
12.10.7.b	Interview & Document Examination	Personnel interviews and records of response actions detailing the adherence to incident response procedures upon the detection of unexpected stored PAN.	1. Can you provide records and personnel testimonials confirming the initiation of incident response procedures upon detecting stored PAN in unexpected locations?

annotations 12 | annotations | requirements | principles | top