# Appendix VIII
# SAS 70 Examinations of EBT Service Organizations

## Background

States must obtain an examination by an independent auditor of the State electronic benefits transfer (EBT) service providers (service organizations) regarding the issuance, redemption, and settlement of benefits under the Supplemental Nutrition Assistance Program (CFDA 10.551) in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No. 70, Service Organizations. Also, States are required to ensure that the service organization has these examinations performed at least annually, that the examinations cover the entire period since the previous examination period, and that the examination reports are submitted to the State within 90 days after the end of the examination period. The examination report must include a list of all States whose systems operate under the same control environment. The auditor of the service organization is required to issue a report on controls placed in operation and tests of operating effectiveness, which is commonly referred to as a "type 2 report" (7 CFR section 274.12(k)(5)).

In performing audits under OMB Circular A-133 of the Supplemental Nutrition Assistance Program, an auditor may use these SAS 70 reports to gain an understanding of internal controls and obtain evidence about the operating effectiveness of controls.

A SAS 70 type 2 report includes a description by the service organization's management of control objectives and related controls as they relate to the services provided, a description by the service organization's auditor of their tests of operating effectiveness and the results of those test, and an auditor's report. This appendix is intended to assist service organizations and their auditors by describing illustrative control objectives and controls that service organizations may have in place. When such controls are present and operating effectively, they may enable auditors of user organizations to assess control risk below the maximum for financial statement assertions related to EBT transactions. The illustrative control objectives and controls in this appendix may not necessarily reflect how a specific service organization considers and implements internal control. Also, this appendix is not a checklist of required controls. Service organizations controls may be properly designed and operating effectively even though some of the controls included in this appendix are not present. Further, service organizations could have other controls operating effectively that have not been included in this appendix. Service organizations and their auditors will need to exercise judgment in determining the most appropriate and cost effective controls in a given environment or circumstance.

Many of the illustrative controls are stated in relation to the kinds of policies and procedures that are "established" or "in place" at an organization. It would be insufficient for such policies and procedures to merely exist on paper and not be implemented. To meet the criteria of a SAS 70 type 2 examination, the policies and procedures would need to be suitably designed, placed in operation, and operating effectively.

## 1. Control Environment

### Illustrative Control Objective:

Controls provide reasonable assurance that the EBT system functions in a manner consistent with its policies, and complies with applicable laws and regulations (Food Stamp Act of 1977, as amended (7 USC 2011 *et seq.*) and 7 CFR section 274.12).

### Illustrative Controls:

- The service organization has written policies and procedures for the system processing EBT transactions.
- The organization identifies and analyzes relevant risks to the EBT process.
- Policies and procedures regarding acceptable employee practices, conflicts of interests, and codes of conduct have been established and communicated to employees with EBT responsibilities.
- Policies and procedures are established for performing background investigations of employees prior to employment.
- Policies and procedures have been established to segregate incompatible functions (e.g., application programming, systems and operation, financial duties, data storage, government reimbursement payment requests, transaction processing, and reconciliation) so no individual interacting with the system can exercise unilateral control over EBT transactions.
- Policies and procedures are in place for management to monitor the effectiveness of EBT controls and correct deficiencies or weaknesses when found.
- Policies and procedures are in place to prevent management or staff from overriding controls.

## 2. Systems Development and Maintenance

### Illustrative Control Objective:

Controls provide reasonable assurance that changes (including emergency procedures) to EBT applications and system software are authorized, tested, approved, implemented, and documented.

**Illustrative Controls:**

- The service organization follows a system development methodology.
- System documentation for new and existing applications are current and complete in accordance with programming and documentation standards used by the service organization.

## 3. Access Controls

**Illustrative Control Objective:**

Controls provide reasonable assurance that the EBT system is protected against unauthorized physical and logical access.

**Illustrative Controls:**

- The responsibility for the development and enforcement of a security policy is at an organizational level that facilitates compliance by service organization personnel and enables enforcement of policies and procedures.
- Security policy and procedures are in place and are communicated to appropriate employees and contractors.
- Policies and procedures are in place for reporting security incidents or observed irregularities to an organizational level where such matters can be investigated and resolved.
- Policies and procedures are established for the security over filing, retention, and destruction of EBT system files.
- Policies and procedures are in place for conducting security system training.
- Policies and procedures are in place for discontinuing an employee or contractor's ability to access EBT hardware, software, and data when the employee is terminated or the employee's duties are changed.
- Access to EBT files or processes is limited based upon users' needs.
- Passwords control access to EBT files, personal identification numbers (PIN), and privacy data.
- Firewalls or other procedures prevent unauthorized access to data from an external network.
- Policies and procedures are in place to prevent a State from reviewing or altering data for another State.

## 4. Computer Operations - Processing

**Illustrative Control Objective:**

Controls provide reasonable assurance that processing is scheduled and deviations from scheduling are identified and resolved.

## 5. Computer Operations - Data Transmission

**Illustrative Control Objective:**

Controls provide reasonable assurance that data transmissions are complete, accurate and secure.

**Illustrative Controls:**

- Policies and procedures require that PINs and data are encrypted throughout processing.
- Encryption keys are stored in a secure manner.
- Maintenance of encryption keys is performed by authorized service center staff.
- Policies and procedures of the service organization require proper identification, validation, and acceptance of EBT transactions processed.

## 6. Computer Operations - Output

**Illustrative Control Objective:**

Controls provide reasonable assurance that output data and documents are complete, accurate, and distributed to authorized recipients on a timely basis.

## 7. EBT Controls - Transactions Received from Authorized Sources

**Illustrative Control Objective:**

Controls provide reasonable assurance that transactions are received from authorized sources.

**Illustrative Controls:**

- Policies and procedures are in place to ensure that updates of point of sale (POS) device parameters are restricted to authorized personnel.
- Policies and procedures require that POS transactions be properly validated.
- Policies and procedures for direct data entry, such as adjustments, require proper review and approval.

- Policies and procedures are in place to approve voucher transactions.

- Policies and procedures for voucher transactions prevent unauthorized access to recipient or retailer accounts.

## 8. EBT Controls - Transaction Amounts and Recording

**Illustrative Control Objective:**

Controls provide reasonable assurance that transactions are for authorized amounts and are recorded completely and accurately.

**Illustrative Controls:**

- Records identify the activity and events in client accounts (e.g., deposits, withdrawals, charges, and type of transactions).

- Records identify client accounts for which benefits have not been withdrawn or used beyond pre-established periods (i.e., identify inactive accounts for which deposits are still made).

- System edits prevent individual client accounts from being credited with benefits in excess of authorized amounts.

## 9. EBT Controls - Processing

**Illustrative Control Objective:**

Controls provide reasonable assurance that transactions are processed completely and accurately.

**Illustrative Controls:**

- Policies and procedures of the service organization include controls to:

  - monitor and investigate any unsuccessful file transfers;
  - recover or reproduce lost or damaged data;
  - examine edit checks for unusual conditions;
  - reconcile input and output of transactions processed;
  - log and store transactions; and
  - monitor rejected transactions and account adjustment actions.

## 10. EBT Controls - Settlement

**Illustrative Control Objective:**

Controls provide reasonable assurance that settlement of funds received from benefit providers and distributed to benefits acquirers for food stamp benefit purchases and withdrawals is performed timely and accurately.

**Illustrative Controls:**

- Policies and procedures are in place to perform daily reconciliations of:
  - account balances;
  - net settlements; and
  - government funds.
- Policies and procedures are established for resolution of disputed transactions.
- Policies and procedures are established for requesting Federal and State reimbursements.

## 11. Physical Environment

**Illustrative Control Objective:**

Controls exist to provide reasonable assurance that physical assets are protected.

**Illustrative Controls:**

- Policies and procedures are established for environmental controls (e.g., maintenance schedules, fire suppression equipment, water detection and protection considerations, and the availability of an uninterruptable power system designed to protect and ensure continued operations).
- Policies and procedures call for periodic facility inspections.
- Policies and procedures for proper maintenance of hardware have been established.

## 12. Contingency Planning

**Illustrative Control Objective:**

Controls exist within the data center to provide reasonable assurance of continuity of operations.

**Illustrative Controls:**

- Disaster recovery and business continuity plans exist for the system processing EBT transactions.

- The business continuity plan provides for periodic testing at the backup facility and the service organization has performed such testing.

- The service organization has a contractually protected access right to the backup facility.

- Backup arrangements for key applications, processes and files are in place.

## 13. Card Controls

**Illustrative Control Objective:**

Controls are established to provide reasonable assurance that users of EBT benefit cards are authorized.

**Illustrative Controls:**

- Each transaction is validated with a unique account number and PIN.

- For benefit card issuance services provided by the EBT service organization policies and procedures are in place to:

  - prevent unauthorized assignment and replacement of PINs;
  - properly deliver benefit cards to participants;
  - activate cards by only authorized users;
  - deactivate damaged, lost, or stolen cards;
  - record and destroy active cards returned to the service organization; and
  - control access to and inventory levels of pre-printed unused card stock.