Data Processing Controls

Processing controls are meant to ensure the reliability of application program processing. An IT auditor should understand the controls exercised over processing to evaluate the exposures covered by them and those that remain. Click the links below to learn more about data processing controls:

Data Validation and Editing Procedures

Data File Control Procedures

Data Validation Edits and Controls

Procedures should be established to ensure that input data are validated and edited as close to the time and point of origination as possible. The chart below outlines various types of data validation edits and controls.

Edits	Description
Sequence check	The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoices begin with 12001 and end with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.
Limit check	Data should not exceed a predetermined amount. For example, payroll checks should not exceed US $4,000. If a check exceeds US $4,000, the data is rejected for further verification/authorization.
Range check	Data should be within a predetermined range of values. For example, product type codes range from 100 to 250. Any code outside this range should be rejected as an invalid product type.
Validity check	Programmed checking of the data validity in accordance with predetermined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, the record should be rejected.
Reasonableness check	Input data are matched to predetermined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives orders for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.
Table lookups	Input data comply with predetermined criteria maintained in a computerized table of possible values. For example, the input clerk enters a city code of 1 to 10. This number corresponds with a computerized table that matches the code to a city name.
Existence check	Data are entered correctly and agree with valid predetermined criteria. For example, a valid transaction code must be entered in the transaction code field.
Key verification	The keying process is repeated by a separate individual using a machine that compares the original keystrokes to the repeated keyed input. For example, the worker number is keyed twice and compared to verify the keying process.

Edits	Description
Check digit	A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors. For example, a check digit is added to an account number so it can be checked for accuracy when it is used.
Completeness check	A field should always contain data rather than zeros or blanks. A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, is present. For example, a worker number on a new employee record is left blank. This is identified as a key field and the record would be rejected, with a request that the field be completed before the record is accepted for processing.
Duplicate check	New transactions are matched to those previously input to ensure that they have not already been entered. For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.
Logical relationship check	If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid. For example, the hire date of an employee may be required to be more than 16 years past his/her date of birth.

Source: *CISA Review Manual, 27th Edition*, USA, 2019, figure 3.18, https://www.isaca.org/bookstore/cisa-exam-resources/crm27ed

Data File Controls

File controls should ensure that only authorized processing is performed on stored data. The chart below provides types of data file controls.

Method	Description
Before and after image reporting	Computer data in a file prior to and after a transaction is processed can be recorded and reported. The before and after images make it possible to trace the impact transactions have on computer records.
Maintenance error reporting and handling	Control procedures should be in place to ensure that all error reports are properly reconciled and corrections are submitted on a timely basis. To ensure SoD, error corrections should be reviewed properly and authorized by personnel who did not initiate the transaction.
Source documentation retention	Source documentation should be retained for an adequate time period to enable retrieval, reconstruction or verification of data. Policies regarding the retention of source documentation should be enforced. Originating departments should maintain copies of source documentation and ensure that only authorized personnel have access. When appropriate, source documentation should be destroyed in a secure, controlled environment.
Internal and external labeling	Internal and external labeling of removable storage media is imperative to ensure that the proper data are loaded for processing. External labels provide the basic level of assurance that the correct data medium is loaded for processing. Internal labels, including file header records, provide assurance that the proper data files are used and allow for automated checking.
Data file security	Data file security controls prevent unauthorized access by unauthorized users that may have access to the application to alter data files. These controls do not provide assurances relating to the validity of data but ensure that unauthorized users who may have access to the application cannot alter stored data improperly.
One-for-one checking	Individual documents agree with a detailed listing of documents processed by the computer. It is necessary to ensure that all documents have been received for processing.
Prerecorded input	Certain information fields are preprinted on blank input forms to reduce initial input errors.
Transaction logs	All transaction input activity is recorded by the computer. A detailed listing, including date of input, time of input, user ID and terminal location, can then be generated to provide an audit trail. It also permits operations personnel to determine which transactions have been posted. This will help to decrease the research time needed to investigate exceptions and decrease recovery time if a system failure occurs.

Method	Description
File updating and maintenance authorization	Proper authorization for file updating and maintenance is necessary to ensure that stored data are safeguarded adequately, correct and up to date. Application programs may contain access restrictions in addition to the overall system access restrictions. The additional security may provide levels of authorization as well as an audit trail of file maintenance.
Parity checking	Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error-detecting or correcting codes. The former is used more often because error-correcting codes are costly to implement and are unable to correct all errors. Generally, error detection methods such as a check bit and redundant transmission are adequate. Redundancy checking is a common error-detection routine. A transmitted block of data containing one or more records or messages is checked for the number of characters or patterns of bits contained in it. If the numbers or patterns do not conform to predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit. Check bits are often added to the transmitted data by the telecommunications control unit and may be applied either horizontally or vertically. These checks are like the parity checks normally applied to data characters within on-premises equipment. A parity check on a single character generally is referred to as a vertical or column check, and a parity check on all the equivalent bits is known as a horizontal, longitudinal or row check. Use of both checks greatly improves the possibilities of detecting a transmission error, which may be missed when either of those checks is used alone.
Version usage	It is critical that the proper version of a file be used as well as the correct file, for processing to be correct. For example, transactions should be applied to the most current database, while restart procedures should use earlier versions.