Chapter 7
Process Domain Information Integrity Enablers and Controls

Overview

Process domain enablers and controls are classified according to the processing life cycle and key components within it that contribute to information integrity.

As discussed in Chapter 4, each process has four main phases – input, processing, output and storage. There are unique sub-phases and repeating sub-phases within each of these phases that contribute to information integrity in specific ways, such as by initiating a routine or procedure, registering/recording/logging the activity performed, matching classifications of the information against access privileges, preventing, detecting and correcting errors, updating metadata, transmitting the information, performing backup and recovery procedures and maintaining the process by managing changes to keep pace with changes in the organization, business processes, etc. All of these, in turn, depend on associated environment domain enablers and controls.

Table 7.1 summarizes the abovementioned phases and sub-phases to illustrate the standard features of an information processing lifecycle.

Table 7.1
Common and Unique Sub-Phases of Processing

	Initiation of phase	Unique Sub-Phases	Registration/ recording/ logging	Matching classifica-tions against access privileges	Error prevention, detection and correction	Assignment/ update of metadata	Trans-mission/ Distribution	Back-up and Recovery	Maintenance and change management
Input	X	1,2	X	X	X	X	X		X
Processing	X	3,4,5,6,7	X	X	X	X		X	X
Output	X	8	X	X	X	X	X		X
Storage	X	9,10	X	X	X	X		X	X

Legend for Unique Sub-Phases

1. Input Capture	6. Updates to perm or semi-perm files, tables, databases
2. Preparation	7. Running applications
3. Aggregating	8. Output display, transmission, distribution
4. Calculations, logic functions and analyses	9. On site/ Offsite Storage
5. Updates to temporary files (e.g. suspense files)	10. Disposal

The following sections discuss the process enablers and controls under four headings – input, processing, output and storage and discusses how various activities and sub-phases contribute to information integrity. The use phase of information processing is not discussed in this section although it is implicit throughout the discussion as the purpose of ensuring information integrity is to provide information that will fit the use for which it was created.

Input Phase

The input phase involves the recognition and capture of relevant content for subsequent processing. Input phase risks arise from the inherent characteristics of various types of input media and data types and the characteristics of input capture procedures and sub-phases.

Types of Input Capture

As noted previously, input can be captured in a variety of ways including:

- Automated input (Sensor based, EDI, RFI, etc.)
- Externally generated by Outsourcers (B2)
- Externally generated by Business (B2B) - Network
- Externally by Consumers (B2C) - Network
- Internal-system generated
- Internal-manually inputted
- Transfer of non-routine (merger, acquisition, other)

Enablers and controls must be sensitive to the type of input capture being used by the entity.

Sub-Phases of the Input Phase

The input phase includes several sub-phases. Illustrative enablers and controls for each sub-phase are identified below.

- Initiation of routine: activities that are required to commence input.
    - Use of automated input devices that reduce or do not require human intervention to commence input.
    - Authorization of transactions converted to machine readable form.
- Input capture/preparation: activities required to gather content for entry
    - Data preparation procedures for user departments are established.
    - Data entry is placed as close to the sources of transactions as possible to ensure familiarity by the transaction initiator with the intention of the transaction.
    - Operating procedures are structured so that business activities cannot be concluded until corresponding transactions are recorded.
    - Suppliers, customers, and other third parties exchange content based upon industry information standards or mutually agreed-upon data/information formats.
    - Outsourcing agreements define the maximum turnaround time for the retrieval of information to meet operational and compliance requirements of the entity.
- Registration/recording/logging: capture of input activities for audit or monitoring.
    - Use of software that logs input activities – time and date of input, user id of inputer
    - Process design that incorporates recording as part of the provision of goods or services (at the boundary between one entity and another); for example: RFID cards for public transit; Telco – creation of CDRs and population of CDR fields during and at end of phone call.
- Matching classifications against access privileges: verifying individuals are authorized to access and approve input related activities.
    - Configuration/settings of access control software are verified periodically against documented procedures.
    - Single sign on is used to manage multiple user IDs and passwords.
- Error prevention, detection and correction: errors or irregularities associated with input are proactively (or reactively) identified and rectified.
    - Input forms/screens incorporate features specifically designed to reduce errors and omissions.
    - The human component in the data entry stage is eliminated to the extent possible.

- Auto-identification technology is used instead of manual entry to capture data.
- Auto-identification devices encode information in a format that adheres to an industry standard or inter-company agreements.
- System matching of documents (e.g., purchase order, receiving report and supplier invoice) is incorporated into the design of information systems.
- Single-source transaction system (e.g., one-write, simultaneous postings, etc.) is used.
- Error correction procedures and responsibilities for errors identified in the input phase are defined.
- Field edits and workflow engines that prevent user from proceeding until completed correctly

- Assignment/update of metadata: metadata associated with input is appropriately assigned or updated.
  - Unique identification is provided for each record to enable tracing of input to output and vice versa.
  - The system is designed to allow the tracing of data backward and forward through the information system.
  - Retention and destruction of source documents, working files, suspense files, intermediary data/documents/authorization forms gathered or generated in the input phase are governed by data retention/destruction policy.
- Transmission: electronic or physical transfer of information from one system to another.
  - Private leased lines or virtual private networking connections with authorized users are used to protect information from unauthorized access, modification, and misaddressing during transmission.
  - Bonded couriers and tamper-resistant packaging are used to protect information from unauthorized access, modification, and misaddressing during delivery.
  - Account activity, subsequent to successful login, is encrypted through industry standard encryption software of sufficient strength to protect web-based input.
  - Date/time stamp and source ID on input transactions to ensure they are submitted by a valid source (i.e. check for: user, terminal, IP address, etc.).
- Maintenance and change management: activities involved in the regular upkeep or changes to the system.
  - Use of automated tools and techniques to identify coding errors (e.g. static analysis tools)
  - Changes made to programs are logged.
- Audit trail: registration/recording/logging of input activities for audit or monitoring.

- Use of software that logs input activities – time and date of input, user id of inputer
- Retain copies of source documents, working files, suspense files, intermediary data/documents/authorization forms gathered or generated in the input phase in accordance with retention policies.
- Provide users with the software capability to scrutinize and analyze data to identify unusual patterns of activity, errors and irregularities.

Processing Phase

As noted previously, the processing phase involves the aggregation or transformation of data into output for display, distribution or storage. Processing phase risks arise from the inherent characteristics of various types of processing activities and the characteristics of processing procedures and sub-phases.

Types of Processing Activities

The processing phase includes several types of activities, including:

- Aggregating data into summarized information
- Performing calculations, logic functions and analyses
- Transforming data or information to an alternative format
- Updating temporary files (e.g. suspense files)
- Updating permanent or semi-permanent files, tables, databases
- Running applications

Enablers and controls must be sensitive to the type of processing performed by the entity.

Sub-Phases of the Processing Phase

In performing these activities, the processing phase includes several activities that are similar to input phase activities. For each of these, illustrative enablers and controls are provided below:

- Initiation of phase: activities that are required to commence processing
    - Skills (training and experience) of employees involved in process match requirements.
- Processing: activities required to transform raw data into semi-processed data or processed output
    - A common standard is used to aggregate/consolidate information that is maintained in disparate systems for reporting or reviewing purposes; e.g. security logs extracted from different systems are mapped to a common standard to analyze trends, policy violations, etc.)
    - Aggregated results permit users to drill down and evaluate components of the aggregated content.
- Registration/recording/logging: capture of processing activities for audit or monitoring.
    - Use of logging software to record transactions entered on-line and internally generated transactions in a log.
- Matching classifications and privileges to permissions for functions/applications: verifying individuals or software agents/programs are authorized to access and approve processing related activities
    - Use of system security software packages, application security features of ERPs (SAP application security, etc.)
    - Reference monitor in applications or infrastructure systems. ERM packages have them and so do operating systems. AD is a common example.
- Error prevention, detection and correction: ensures that errors or irregularities associated with processing are proactively (or reactively) identified and rectified
    - Downstream systems prevent the incomplete or inaccurate capture of content from upstream systems. Processing can only occur once any information integrity issues that are identified have been resolved.
    - Downstream users aggregate information from upstream users in manner that recognizes the underlying data elements that are used to construct the information (e.g. the marketing department uses sales data from the financial system with an understanding of how that information was created, its sources and limitations.)

    - Error correction procedures and responsibilities for errors identified in the processing phase are defined.
    - Independent review or monitoring of transaction processing.
- Assignment/update of metadata: metadata associated with semi-processed or processed data is appropriately assigned or updated.
    - When a process transforms inputs into outputs that are not directly traceable back to the inputs, reconciliation procedures are designed into the process and there is sufficient documentation of the transformation routine(s) to enable tracing input to output, and vice versa.
    - Source documents, working files, suspense files, intermediary data/documents/authorization forms gathered or generated in the processing phase are retained in accordance with the retention policy.
- Transmission: electronic or physical transfer of information from one system to another.
    - Common standards are used for data exchange between entities.
    - ERPs (where data is stored once and used by all the system modules of the ERP) and/or data base management systems are used.
    - Skills of employees responsible for the physical transfer of data.
    - Features of devices used in electronic and physical transfer.
- Backup and recovery: activities related to securely storing data for the purpose of recovery in the event of data loss during processing, including those copies sent offsite
    - Entity level data architecture that identified the archive requirements for each data set.
    - Skills (training and experience) of employees at off-site location.
- Maintenance and change management: activities involved in the regular upkeep or changes to the system.
    - Revision control and source code management software or service is used by programmers to make changes.
    - Skills of programmers/end-users making the changes.

Output Phase

The output phase is the culmination of the processing phase that transforms processing results into information and displays or distributes it to users of the information. The distribution or delivery phase may be an identifiable and separate sub-phase of the output phase, particularly when output

is produced for storage in a database or data warehouse and users access the output through query facilities. Output phase risks arise from the inherent characteristics of various types of output media and output types as well as the characteristics of output procedures and sub-phases.

Types of Output

As noted previously, output can be provided in a variety of ways including:

- Scheduled output, reporting, abstraction, and summarization
- Ad hoc reporting based on query tools
- Data mining outputs
- Manual end user collation
- Output to Consumer
- Output to Business
- Output to system
- Output to manual process
- System generated output (e.g. purchase)
- Output over network

Enablers and controls must be sensitive to the types of output produced by the entity.

Sub-Phases of the Output Phase

The output phase includes several activities that are similar to input and processing phase activities:

- Initiation of phase: activities that are required to commence output

    - Skills (training and experience) of employees involved in the process match requirements..

- Output: activities related to transforming processed data into usable information (e.g. a report, spreadsheet, statistics, etc.).
    - Reporting and query tools are able to extract and aggregate information in a timely manner to meet operational and compliance requirements.
- Retrieval: activities related to retrieving or extracting processed data from a repository
    - Reporting and query tools ensure that information is complete and current and is extracted from authorized storage areas.
- Registration/recording/logging: capture of output activities for audit or monitoring.
    - Physical media (e.g. paper, discs, etc.) are labelled with the information integrity classification and are handled by users who are authorized to access such material.
    - Periodically copy and save permanent records which are changed by overwriting the old contents in the same physical storage location.
- Matching classifications and privileges to permissions for access: verifying individuals or software agents/programs are authorized to access and approve output related activities
    - Reference monitor in applications or infrastructure systems. All the ERM packages have them and so do the operating systems. AD is a common example
    - Security software packages such as RACF, application security features of ERPs (SAP application security, etc.)
- Error prevention, detection and correction: ensures that errors or irregularities associated with output are proactively (or reactively) identified and rectified
    - Error correction procedures and responsibilities for errors identified in the output phase are defined.
- Assignment/update of metadata: metadata associated with output is appropriately assigned or updated
    - Output provides cross-referencing to the inputs that it is based on so that summary figures can be traced back to the source inputs.
    - Unstructured content that is meant to be retrieved through searches is labelled in accordance with standards that enable timely retrieval of information.

    - Retention and destruction of source documents, working files, suspense files, intermediary data/documents/authorization forms gathered or generated in the output phase is governed by data retention/destruction policy.

- Maintenance and change management: activities involved in the regular upkeep or changes to the system.
    - Changes in the underlying data structures (database, data warehouse, etc.) are assessed for impacts on routine outputs. Where impacts are identified, appropriate changes are made to user reports.

- Transmission: electronic or physical transfer of information from one system to another.
    - LAN and WAN are stable.
    - ERPs (where data is stored once and used by all the system modules of the ERP), data base management systems are used.
    - Skills of employees responsible for the physical transfer of data match requirements.
    - Features of devices used in electronic and physical transfer match requirements.

Storage Phase

The storage phase is one of the endpoints of the processing phase whereby information is stored for subsequent access. The storage phase includes short term working storage, medium term storage and long-term archival storage. Thus, the storage phase may be used to hold inputs until they are processed, tables, files and databases used by application programs and backups and archives for subsequent access if required. The disposal phase may be an identifiable and separate sub-phase of the storage phase, particularly when stored information must be disposed of in a prescribed manner pursuant to security requirements or laws and regulations such as those pertaining to personal information. Storage phase enablers include the inherent characteristics of various types of storage media and the characteristics of storage procedures and sub-phases.

Types of Storage

As noted previously, the storage phase of processing can involve all kinds of media and a variety of data:

- Databases, including ERP

- Data warehouse, datamarts
- Desk and filing cabinets
- Archives
- Short term storage files, tables, and databases (i.e. readily accessible)
- Intermediate storage in various physical/logical storages (e.g. onsite tape libraries)
- Long term storage in data warehouse, master database
- Structured data vs unstructured data
- Relational database vs flat file
- Disk vs tape vs USB
- Encrypted vs clear text

Enablers and controls must be sensitive to the types of storage data and media used by the entity.

Sub-Phases of the Storage Phase

Storage phase risks arise from the inherent characteristics of various types of storage media and the characteristics of storage procedures and sub-phases.

- Initiation of phase: activities that are required to commence storage.
    - Data classification and labelling policy.
    - Skills (training and experience) of employees.
- Registration/recording/logging: capture of storage activities for audit or monitoring.
    - Unique identification is provided for each record.
    - Data classification and labelling policy.
    - Use of logging software.

- Matching classifications against access privileges: verifying individuals or software agents/program are authorized to access and approve storage related activities.
    - Reference monitor in applications or infrastructure systems. All the ERM packages have them and so do the operating systems. AD is a common example.
    - Use of system security software packages such as RACF, application security features of ERPs (SAP application security, etc.).
- Error prevention, detection and correction: ensures that errors or irregularities associated with storage are proactively (or reactively) identified and rectified.
    - Entity level data architecture that identified the archive requirements for each data set.
    - Storage environment (humidity, temperature, dust free, etc.) helps maintain the integrity of the storage media.
- Assignment/update of metadata: metadata associated with stored data is appropriately assigned or updated.
    - Unique identification is provided for each record.
- Retention in onsite/offsite storage: activities to ensure that information (and the media it resides upon) is retained for a period of time that reflects the operational, statutory, and regulatory requirements of the entity.
    - Retention and destruction of source documents, working files, suspense files, intermediary data/documents/authorization forms gathered or generated in the storage phase are governed by data retention/destruction policy.
    - Record retention procedures are documented.
    - Automated procedures exist to automatically migrate data from a working/short-term repository to long-term storage.
    - Skills (training and experience) of employees match requirements.
    - Each record is filed in a significant and planned sequence to facilitate retrieval.
    - Data classification and labelling policy matches requirements. The retention period takes into account the risk of unauthorized access to the content the longer it is retained.
    - Data/Information content is maintained in a centralized repository that is independent of the application system(s).
- Backup and recovery: activities with storing/restoring processed output, including those activities pertaining to offsite storage, restoration and testing:

    - Entity level data architecture that identified the archive requirements for each data set
    - Existence of written back-up and recovery policies and procedures related to storing and restoring of back-up. Skills (training and experience) of people involved in the back-up and recovery process. Reliability of the software used to create back-up.
    - Access to encryption keys or other tools to read or access the software.

- Maintenance and change management: activities involved in the regular upkeep or changes to the system.
    - Use of change management software.

- Disposal: destruction of data (or the medium that stores the data) to the point that the data is not accessible or usable.
    - Entity level data architecture identified the archive requirements for each data set.
    - Reliability of devices used to destroy media used to store data matches requirements.
    - Skills of people involved in the destruction process match requirements.

Link to IS Environment and Content Domains

Enablers and controls in the process domain depend on the effective functioning of enablers and controls in the IS environment domain. That is, the effective functioning of enablers and controls within processing phases and sub-phases depends on the effectiveness of the IS environment domain enablers and controls discussed in the previous chapter.

Similarly, enablers and controls in the content domain discussed in the next chapter depend on both the process enablers and controls discussed in this chapter and the IS environment domain enablers and controls discussed in the previous chapter.