Chapter 6
IS Environment Domain Information Integrity Enablers and Controls

Overview

As was discussed earlier, IS environment domain enablers and controls fall into the following eight categories of activities:

1. information governance practices,
2. information creation practices aimed at achieving fit for purpose and understandability of the information,
3. security practices to protect the information against unauthorized creation, change and destruction,
4. availability processes to ensure the information is available to and accessible by authorized users,
5. dependability practices to ensure predictable operation,
6. standards to ensure consistency of information production,
7. verifiability features to enable verification of information integrity and
8. assurance services to add credibility to assertions about information integrity.

For each of these categories of enablers and controls, key activities that contribute to information integrity are identified below.

Code	Phase	ITCG Ref, if applicable	Frequency in ITCG 1998	Frequency in this Publication
ITG	**Information Governance**			
ITG-01	Adopt a Strategic Perspective on Information Integrity	C1,C2, C4, D1-D5, E2-E5, F1, F2, F4	54	
ITG-03a	Assign Responsibility and Accountability for the Management and Support of Information Integrity			
ITG-03b	Address Human Resource Issues and Barriers to Implementing Information Integrity			
ITG-04	Implement Information Integrity Program(s)	Q1-Q2, R1-R3,	30	
ITG-02	Prioritize Action Plans Based on Risk Assessment	A1-A3, B1-B5, B7	21	
ITG-05	Monitor Information Integrity and Implement Required Changes in Governance	B6, C3, E1, F3, G1-G3	30	
DES	**Definition, Design, Development and Deployment to Achieve Fit for Purpose**			
DES-01	Adopt a System Development Life Cycle (SDLC) at a Suitable Level of Maturity/Quality	H1-H4	15	
DES-02 02a	Project Management	I1-I5	21	
DES-03 02b	Establish Project Management Practices	J1-J7, AA1-AA3	44	
DES-03	Identify Information Requirements			
DES-04	Acquire and/or Develop Process Components	K1-K6	30	
DES-05	Implement Process to Produce Information	L1-L12	46	
DES-06	Maintain System and Manage Change	M1-M9	32	
DES-07	Manage User Developed Applications	S1-S4	24	
DES-08	Monitor SDLC Quality, Identify Required Changes and Manage Change Process	K5, K5-1	2	
SEC	**Security – Access control and asset safeguarding**			
SEC-01	Establish Responsibility and Accountability for Security	T12 (physical access only)	2	
SEC-02	Establish Environment and System Boundary Controls	Q1-Q4, T1	32	
SEC-03	Classify Information Assets According to their Sensitivity/Value	T5-T6	9	
SEC-04	Assess Risks	T2	7	

Code	Phase	ITCG Ref, if applicable	Frequency in ITCG 1998	Frequency in this Publication
SEC-05	Establish Security Policies, Standards and Guidelines to Address Risks	X1	4	
SEC-06	Ensure Personnel Have Required Qualifications and are Trustworthy	T11, W1-W2	12	
SEC-07	Implement Information and Communication Program to Raise Security Awareness	X2	3	
SEC-08	Analyze User Access Requirements and Manage Privileges	T7-T8	10	
SEC-09	Implement Physical Access Controls	O7, T13	10	
SEC-10	Implement Logical Access Controls and Segregation of Incompatible Functions	M8, O7, T4, T9, U1-U3	30	
SEC-11	Manage Operations and Monitor Vulnerabilities • Intrusion Detection and Incident Response • Vulnerability Management – Design/Architecture • Vulnerability Management - IT Environment and Component Quality	P4, T3	19	
SEC-12	Verify Procedural Compliance	X3	3	
SEC-13	Monitor Non-Compliance and Take Appropriate Remedial Action	M8, T10	7	
AVA	**Availability/Accessibility**			
AVA-01	Establish Responsibility and Accountability for Availability/Accessibility	Y1, Z2	9	
AVA-02	Implement IT Environment Controls	O4, V1-V3	20	
AVA-03	Perform Routine Back-up & Recovery	O2	8	
AVA-04	Plan for System Continuity	Y1-Y2,Y5, Y6 (like O5)	20	
AVA-05	System Continuity Planning	O5, O8, Z1-Z2, Z5, Z6 (like O5)	36	
AVA-06	Insurance			
AVA-07	Monitor Information Availability Statistics and Make Required Changes	Y3-Y4, Z3-Z4	30	
DEP	**Dependability/Reliability**			
DEP-01	Plan Capacity and Acquire and/or Develop Infrastructure	P2	13	
DEP-02	Implement Service Level Agreements	N1	16	
DEP-03	Implement Operations Controls	O1, O3, O6 (like N2), Q3	14	

Code	Phase	ITCG Ref, if applicable	Frequency in ITCG 1998	Frequency in this Publication
DEP-04	Manage Configuration and Version Controls	N5, N7, P1, Q4 (same as R4)	24	
DEP-05	Monitor Dependability of Information Processing, and Make Required Changes	N2-N4, N6, P3	27	
CON	**Standards/Consistency**			
CON-01	Establish Standards	R4	4	
CON-02	Verify Compliance with Standards			
CON-03	Monitor Non-Compliance and Take Remedial Action			
AUD	**Verifiability/Auditability**			
AUD-01	Establish Audit Trails	EE1-EE4, EE6	25	
AUD-02	Establish Data/Information Retention and Disposal Policies	EE5	1	
	Define information integrity measurement processes and rules			
AUD-03	Acquire Audit Tools			
AUD-04	Monitor Identified Gaps and Implement Changes to Eliminate Those Gaps			
CRE	**Assurance/Credibility**			
CRE-01	Implement an Information Integrity Assurance Program			
CRE-02	Have Internal Audit Provide Periodic Assurance on Information Integrity			
CRE-03	Have External Audit Provide Periodic Assurance on Information Integrity			
CRE-04	Monitor Information Integrity Assurance Outcomes, Learn From Them and Implement Required Changes			

Information Governance

Information governance can help to ensure that an entity adopts a strategic perspective on information integrity, addresses human resource issues and other barriers to the implementation of an effective information integrity program, prioritizes activities on the basis of risk assessment and monitors the effectiveness of those activities, adapting them as necessary. There are several key activities related to this enabler:

- Adopt a Strategic Perspective on Information Integrity
- Assign Responsibility and Accountability for the Management and Support of Information Integrity

- Address Human Resource Issues and Barriers to Implementing Information Integrity
- Implement Information Integrity Program(s)
- Prioritize Action Plans Based on Risk Assessment
- Monitor Information Integrity and Implement Required Changes in Governance

Each of these aspects is discussed below.

Adopting A Strategic Perspective On Information Integrity

- Treat information production processes as strategic assets or investments rather than as operating expenses—Management relies on information to plan and monitor entity activities and to make strategic decisions. Accordingly, management should treat activities that ensure information integrity as being strategically important as well. This means treating information production processes as strategic assets or investments rather than viewing them as operating expenses. Treating information systems and operations as an expense rather than an investment, emphasizes short-term gains through cost reductions to the detriment of information integrity. A long-term "investment" perspective results in allocation of necessary funding and other resources that will support the achievement of an entity's information integrity objectives.

- Define and prioritize the information integrity objectives for key categories of information—Since it is not possible to achieve a 100% level of information integrity, and due to the inherent limitation of resources within an organization the enterprise must define information integrity objectives for its key categories of information and prioritize the information integrity objectives for its key categories of information.

Assigning Responsibility and Accountability for the Management and Support of Information Integrity

- The entity's information integrity management framework should address management roles and responsibility for the reliable maintenance of operations, integrity standards, production, and distribution of information.

- Define responsibility and accountability for the information assets—A clear definition of responsibility and accountability for information is required to focus attention on information integrity management and identify which organizational units and people are designated "owners" or "stewards" and "custodians" of various information sets. (e.g., business unit manager is owner and DBA is custodian). In practice accountabilities are often spread broadly (e.g. a data architecture function will have accountability for data standards, the business unit will be accountable for accuracy of input and database systems professionals will ensure secure access).

- Establish information integrity policies and standards—Standards need to be codified and communicated for organizations to be able to measure the quality of their information and guide their employees to adhere to best "information integrity" practices. Applying total quality management (TQM) ideas from the manufacturing experience to the world of information quality implies that the goal is to meet the needs of "information users" consistently.

- Provide leadership or tone at the top—Management needs to be the driver and key initiator of any information integrity program.

Addressing Human Resource Issues And Barriers To Implementing Information Integrity

- Establish human resource policies—Organizations should assess the human resource issues that surround the data entry, processing and output processes to motivate personnel to pay attention to information integrity and eliminate any barriers preventing personnel from taking actions to improve information integrity.
- Motivate integrity—Organizations should motivate personnel to pay attention to information integrity and eliminate barriers preventing personnel from taking actions to improve information integrity. This includes a combination of communications and incentives.

Implementing Information Integrity Program

- Design an information integrity management process—This includes defining a distinct role for information integrity management, identifying users' requirements and creating a governance process explicitly focussed on information integrity. Such a role should also have an end-to-end understanding of the entire process and should be able to monitor/identify gaps between departments or sub-processes.
- Implement controls—This includes re-engineering processes to establish control points, eliminating trouble spots, automating processes to eliminate error generators and embedding error detection and correction processes.

Prioritizing Activities Based on Risk Assessment

- Establish or adopt a Risk Assessment Framework
- Establish an inventory of projects or areas requiring assessment in each of the three domains: content, process and environment.

- Assess risks, costs and operational losses
- Prioritize over an appropriate time horizon to obtain optimal reduction of risk per unit of cost

Monitoring, Learning and Change Management

- Establish metrics—Measure the results of the information integrity initiatives.
- Identify information integrity problems and issues—A combination of manual and automated approaches should be used to identify problems.
- Evaluate and report findings—Findings should identify causes of impairments, specific organizational impacts and costs.
- Make changes based on findings.

Definition/Design/Development/Deployment to Achieve Fit for Purpose

As noted earlier, fitness-for-purpose is a pre-requisite for information integrity since the four core attributes of information integrity must be judged in light of the purpose that the information is intended to serve. Fitness-for-purpose depends on effective design, development and deployment of a process and related information to achieve an appropriate level of granularity or aggregation clarity, understandability and transparency. This enabler includes the following key activities:

- Adopt a System Development Life Cycle (SDLC) at a Suitable Level of Maturity/Quality
- Establish Project Management Practices
- Identify Information Requirements
- Acquire and/or Develop Process Components
- Implement Process to Produce Information
- Maintain System and Manage Change
- Manage User Developed Applications
- Monitor SDLC Quality, Identify Required Changes and Manage Change Process

Many factors can contribute to the understandability and transparency of information, including user knowledge, skill, training and motivation. In addition, information design choices such as its level of aggregation (or granularity) will affect its understandability/ transparency, hence, the ability of users to assess its level of information integrity. For some purposes, highly aggregated information may be called for; whereas for other purposes, very detailed information may be required. Thus, appropriately tailored levels of granularity/aggregation can be enablers of information integrity. A proxy for the transparency/understandability of information is its conformity with user-specified requirements.

Security Access Control and Asset Safeguarding

Access restrictions and safeguarding practices can help to protect information against unauthorized creation, change and destruction. The security practices enabler includes the following key activities:

- Establish Responsibility and Accountability for Security
- Establish Environment and System Boundary Controls
- Classify Information Assets According to their Sensitivity/Value
- Assess Risks
- Establish Security Policies, Standards and Guidelines to Address Risks
- Ensure Personnel Have Required Qualifications and are Trustworthy
- Implement Information and Communication Program to Raise Security Awareness
- Analyze User Access Requirements and Manage Privileges
- Implement Physical Access Controls
- Implement Logical Access Controls and Segregation of Incompatible Functions
- Manage Operations and Monitor Vulnerabilities
- Verify Procedural Compliance
- Monitor Non-Compliance and Take Appropriate Remedial Action

Physical and logical access controls and safeguards over information in motion and at rest are required to protect information against inadvertent errors that could compromise its integrity, acts of nature and intentional malicious acts such as unauthorized creation, modification or destruction.

Exclusion of Confidentiality/Privacy

An important aspect of security involves protecting the confidentiality of information or privacy of personal information; that is, protecting it against unauthorized viewing, use or dissemination. Many security controls serve to simultaneously protect information against threats to representational faithfulness from unauthorized creation, tampering or deletion of information and threats to confidentiality and privacy from unauthorized viewing, use or disclosure of information. Some parties may view a breach of information confidentiality as a breach of integrity.

While confidentiality and privacy are important aspects of security, they are conceptually different from the concept of *representational faithfulness* and are not explicitly addressed in this publication.

Availability

Access management and environmental protection procedures can help to ensure the information is available to and accessible by authorized users. The availability enabler includes the following key activities:

- Establish Responsibility and Accountability for Availability/Accessibility
- Implement IT Environment Controls
- Perform Routine Back-up & Recovery
- Plan for System Continuity
- Insurance
- Monitor Information Availability Statistics and Make Required Changes

Information needs to be available and accessible to users in accordance with business specifications and to be in a usable form when required (i.e., locatable, retrievable, presentable, and interpretable). Information that is not accessible when needed would not have any practical consequences for users' activities or decisions, except in the negative sense of limiting the quality of the information and users' decisions based on that information. For information to be deemed accessible, users need to be able to work with the information in a way that meets their needs.

The storage phase of processing is most closely associated with this environmental enabler. Practically, this requires the use of a robust process that makes content available when it is needed.

Security and availability procedures are complementary in the sense that procedures labelled as security procedures aim to prevent unauthorized access to information whereas procedures labelled as availability procedures aim to facilitate authorized access to information.

Dependability

Effective operations practices can help to ensure predictability of operations. The dependability enabler includes the following key activities:

- Plan Capacity and Acquire and/or Develop Infrastructure
- Implement Service Level Agreements
- Implement Operations Controls
- Manage Configuration and Version Controls
- Monitor Dependability of Information Processing, and Make Required Changes

Several similar, but not identical, characteristics are often grouped together under this heading, including: dependability, repeatability; stability and predictability. Although they have subtle differences, they are treated as synonyms in this publication. The dependability of information is facilitated by consistency in how information is measured and presented or displayed to decision makers, the predictability of information processing and the predictability of the events that the information systems are designed to process information about. Events may be inherently unpredictable, but the information about them need not be. For example, a baseball player may not hit a home run each time at bat because athletic performance is unpredictable, but the information about the baseball player's performance may be dependable because there is a well-defined measurement protocol for observing and recording that information. To the extent that dependability is the result of a consistent measurement protocol or a predictable information process or system, the representational faithfulness of information will depend both on the reliability of the process and the reliability of related change management processes applied to the protocol, process or system.

Standards

Standards can help to ensure consistency of information production. The standards enabler includes the following key activities:

- Establish Standards
- Verify Compliance with Standards
- Monitor Non-Compliance and Take Remedial Action

The definition and enforcement of information integrity standards supports the spatial, temporal and relational consistency of information production:. Environmental uncertainties perturb information systems and can lead to changes that can adversely affect stability and consistency and, hence, their comparability. Examples of such environmental factors include complexity (e.g., a system incorporates the use of new interfaces with external entities), change (e.g., regulatory changes), IT devices and computer crime (e.g., hacking) (Nayar, 1996). Standards such as measurement and presentation rules, business policies and legal requirements represent the basis for consistent treatment of information over time, across systems and across decision contexts.

Verifiability

Features such as audit trails, audit tools and human resources enable monitoring and verification of information integrity. The verifiability enabler and control includes the following key activities:

- Establish Audit Trails
- Establish Data/Information Retention and Disposal Policies
- Define information integrity measurement processes and rules
- Acquire Audit Tools
- Monitor Identified Gaps and Implement Changes to Eliminate Those Gaps

Verifiability is the ability of independent observers, applying the same processes and tolerances to the evaluation of selected criteria such as completeness, currency, accuracy and validity that are used to produce the information, to replicate substantially the same result. In this publication, the concept of verifiability is considered to subsume the concept of neutrality (freedom from bias). In order to verify and communicate information integrity to parties external to the information process, the core components of integrity verification need to be defined, objective and

measurable. This implies an approved or agreed upon set of processes or measurement rules, otherwise it would be difficult to obtain the consensus that verifiability requires. In a business context, the approved set of processes or measurement rules springs from Board-approved policies and standards and applicable legal, regulatory or professional requirements. Among other things, these must define the degree of tolerable imperfection in information integrity (in the assurance literature, also termed precision or tolerable error) for core attributes of completeness, currency, accuracy and validity, as further discussed in the section on the importance of context.

Verifiability features make it possible to trace information back to its source and confirm its representational faithfulness. Key features include unique content or information identifiers such as a unique document or transaction identification number, creation date and modification date time stamps, identification of the source content and collection method, information retention and archiving, accessibility information and unambiguous and clearly documented re-computation rules.

Assurance

Internal and external assurance services can add credibility to assertions about information integrity. The assurance enabler of information integrity includes the following key activities:

- Implement an Information Integrity Assurance Program
- Have Internal Audit Provide Periodic Assurance on Information Integrity
- Have External Audit Provide Periodic Assurance on Information Integrity
- Monitor Information Integrity Assurance Outcomes, Learn From Them and Implement Required Changes

The intangible nature of information may prevent direct physical observation of information's integrity and, therefore, it may only be verified through indirect measures. In addition, parties external to the information may only be able to ascertain the integrity of information if they, or their agents, can obtain audit assurance from an independent, objective third party regarding the various attributes of information.

The intangibility of information may limit the ability of users to assess information to determine whether or not it has integrity. For information integrity to be trusted, there must be evidence that

it has been safeguarded against forgery or tampering by unauthorized parties. While verifiability represents a necessary condition for obtaining assurance about information integrity, credibility stems from audit procedures that are actually performed to verify the integrity of the information by gathering evidence about its representational faithfulness.

Link to Process and Content Domains

The information integrity of both content and the process it is used in are determined by their environment. IS environment domain enablers help to ensure that process and content integrity are given priority, that they fit their purpose, are protected against unauthorized access while being accessible to authorized users, operate dependably and consistently, are verifiable and assured.