# Chapter 5 IS Environment Domain Risks

## *Overview*

Example risk statement – The IS Environment fails to effectively ensure that underlying processes are designed, operated and maintained completely, accurately, promptly and in an authorized manner.

Flaws in the creation, operation and change in features of the IS environment can result in an environment that does not have appropriate information integrity enablers and controls. This in turn can create information integrity impairments for processes that depend on the environment, the metadata that depend on those processes and the content that depends on all of them. Complexity increases these risks.

An IS environment that contains the following categories of enablers and controls increases the likelihood that the processes and the content handled by those processes will have an acceptable level of information integrity:

1. Information Governance practices,

2. Fit for Purpose - Design, development and deployment practices that ensure process and content fit for purpose (relevance, clarity, understandability, appropriate level of granularity, appropriate level of aggregation),

3. Security – Access control and safeguarding practices to protect the information against unauthorized creation, change and destruction,

4. Availability/ Accessibility – Practices to ensure the information is available to and accessible by authorized users,

5. Dependability - Practices to ensure predictability of operations,

6. Consistency – Standards to ensure consistency of information production,

7. Verifiability – Features such as audit trails, audit tools and human resources to enable verification of information integrity, and

8. Assurance – Internal and external services to add credibility to assertions about information integrity.

## *Information Governance*

A key enabler of information integrity is 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. Essentially, the leadership views information as an investment instead of an expense.

Threats to the effectiveness of information governance include problems with tone at the top such as failing to give information integrity priority, failing to define responsibility and accountability for information integrity, limitations in the design of information integrity policies, standards, benchmarks and mechanisms, failure to align information governance activities with business strategy and business risks, failure to maintain a comprehensive inventory of information integrity risks and related controls, inconsistent communication of information integrity policies or failure to implement and enforce procedures that implement those policies, and failure to adapt to changes in the business environment, business strategy or organizational structures.

## *Creation Practices That Result in Fit for Purpose*

Definition, design, development and deployment practices can help ensure processes and content are fit for their intended purpose (i.e., they have clarity, understandability, appropriate level of granularity, and appropriate level of aggregation).

Threats to fitness-for-purpose include limitations in the system development lifecycle that result in incomplete or inaccurate information integrity requirements, flaws in design or operation of information integrity enablers and failure to adapt requirements, features or operations procedures

to organizational or environmental changes. As user developed applications are (usually) not subject to the same rigour as professional computing, it represents a particular challenge in this regard.

### *Security*

Access restrictions and safeguarding practices can help to protect information against unauthorized creation, change and destruction.

Threats to security include failure to establish an effective chain of authority, responsibility and accountability for security, failure to define and implement effective boundary protection, failure to identify sensitive information assets requiring strong access restrictions, failure to match level of access protection to the level of risk, failure to define and document security policies, standards and guidelines, failure to ensure that personnel are qualified, trustworthy and informed about security, failure to implement physical and logical access restrictions, failure to implement effective procedures for monitoring vulnerabilities, incidents and compliance with established policies and failure to adapt security specifications in response to organizational and environmental changes.

### *Availability/Accessibility*

Access management and environmental protection procedures can help to ensure the information is available to and accessible by authorized users.

Threats to availability include failure to establish an effective chain of authority, responsibility and accountability for availability and accessibility, failure to define and implement an effective system continuity plan, including effective IT environment protection and routine back-up and recovery measures and failure to adapt availability specifications in response to organizational and environmental changes.

### *Dependability*

Operations practices can help to ensure predictability of operations.

Threats to dependability include failure to establish an effective IT infrastructure that is aligned with the risks assessed, failure to specify and monitor service levels, failure to implement effective operations procedures and configurations and failure to adapt operations in response to organizational and environmental changes.

### *Consistency*

Standards can help to ensure consistency of information production.

Threats to consistency include failure to define, implement and monitor compliance with effective standards and failure to adapt standards in response to organizational and environmental changes.

### *Verifiability*

Features such as audit trails, audit tools and human resources enable monitoring and verification of information integrity.

Threats to verifiability include failure to implement comprehensive audit trails, failure to establish retention and disposal requirements, failure to obtain the tools and personnel required to monitor and verify compliance and failure to adapt audit trails, retention and disposal requirements in response to organizational and environmental changes.

### *Assurance*

Internal and external assurance services can add credibility to assertions about information integrity.

Threats to assurance include failure to define and implement a comprehensive assurance program for information integrity (e.g., focusing on procedures and omitting assessments of policies or the risk assessment program), failure to establish information integrity assurance mandates and priorities for the internal and external auditor(s), failure to monitor scope and quality of assurance practices, inadequate use of automated testing procedures and failure to adapt assurance requirements in response to organizational and environmental changes.

Another risk associated with assurance is failure to remediate the problems identified by the assurance program.

Table 5.1 summarizes information integrity risks by environment domain enabler.

## *Risk Magnifiers*

### Complexity

Complexity factors that may magnify risks in the environment domain include:

1. **Information Governance**
    - Multiple (i.e. in terms of variety and number) business lines, organizational units, languages.
    - Multiple objectives, risk factors and factors for prioritizing may lead to conflicting priorities.
    - Multiple quality metrics, multiple trade-offs between completeness, currency, accuracy and validity
    - Regulatory or industry volatility
2. **Definition, Design, Development, Deployment of Processes and Content to Achieve Fit for Purpose -**
    - Multiple phases of SDLC and multiple levels of maturity.
    - Multiple sources of service.
    - Multiple phases; resource limitations; deadlines
    - Multiple users and uses of information; uncertainties about best information formats for new systems
    - Development project initiation issues.
        - Project sponsorship
        - Business commitment to the change initiative
        - Scope of the change initiative
        - Complexity of the business requirements of the project
        - Complexity of the technical requirements
        - Number and degree of business organizations, processes and policies required to be changed
        - Number of system interfaces

    - Reliance on outsourced services
- Development project execution issues.
    - Number of estimated effort hours
    - Project duration
    - Newness of the project technology
    - Subject matter expertise available to the project team
    - Dependency on other projects or teams
    - Reliance on outsourced services
- Project management experience and knowledge
    - Project team familiarity with the project management methodology
    - Availability of people to work on the project
    - Project team location(s)
    - Amount of customization needed to packaged solutions
    - Experience and stability of the solution vendor
    - Ability to test the new system(s)
    - Implementation strategy – phased implementation or 'big bang'
- Multiple systems; competing demands for maintenance; conflicting views on needed changes
- Large number of users with limited IS skills
- Tension between IS and Internal Audit

**3. Security**

- Multiple access protocols e.g. wireline, wireless, dial up, etc.
- Multiple information asset types with varying criticality/sensitivity depending on class of user and nature of use.
- Subjective judgments about nature of threats, their probabilities and consequences.
- Human factors may create barriers to effective communication.
- Variety of parties with varying privileges to access data; numerous access points, types of equipment, facilities, media, and processing - inhouse and outsourced; online and offline; onsite and offsite.
- Multiple sources of intruders
- Balance productivity and intrusiveness.

4. **Availability**
    - All critical user departments, business processes and system components – facilities, equipment, data (including devices and media), people, procedures must be identified.
    - Unpredictable events.
    - Outsourced services.
5. **Dependability**
    - Numerous devices, varying volumes
    - Variety of configuration options
    - Internal and external processing may be difficult to co-ordinate.
    - Scheduling
6. **Consistency - Standards**
    - Variety of standards may be adopted by business units.
    - Difficult to establish priorities for compliance verification.
7. **Verifiability**
    - Difficult to create audit trail that spans multiple business units and business processes.
    - Numerous business units and process in multiple jurisdictions require comprehensive retention policies that satisfy entity requirements, audit requirements and legal/regulatory requirements.
    - Variety of tools and service providers. Few end-to-end tools/services.
8. **Assurance**
    - Fraud falls below audit thresholds (e.g. Salami technique)
    - Conflicting priorities between operational and financial auditing.
    - Conflicting priorities between security administration and internal audit.
    - Conflicting responsibilities between internal and external audit.

## Inherent Nature

The inherent nature of aspects of the environment may magnify risks in the environment domain include:

- Size: larger organizations inherently face more issues than smaller organizations (e.g. more to coordinate, more to secure, etc.)

- Volatility: economic sectors or environments with rapidly changing information are more risky than stable sectors or environments

- Socio-economic region: some regions are more unstable than others. For example, establishing a data center in politically unstable region (e.g. due to volatile socio-economic conditions) is inherently more risky than having a data center in a politically stable region.

- Regulatory/legal scrutiny: the more regulated an organization is, the higher the risk of facing regulatory sanction.

- First adopters: adopting new, untested processes or technologies can impose additional risks, as many unknowns exist that can negatively impact the environment.

- Climatic conditions: certain locations impose additional risks on an environment (e.g. areas prone to earthquakes, hurricanes, high humidity, etc.)

- Degree of non-physicality: Businesses that deal with virtual goods (i.e. that lack physical existence) are more disrupted by system failures (e.g. telecomm companies deliver service virtually and receive billing information electronically, where as a manufacturing company deliver physical goods that can be handled outside the system).

## Malicious Intent

Unintentional flaws in the environment may impair the information integrity of processes and content used in the environment.

Information integrity may also be impacted by the deliberate creation of an environment that permits tampering with information processing and content.

Table 5.1 illustrates some of the risks by enabler and risk category.

**Table 5.1 Information Risks by IS Environment Enabler**

| | **Illustrative Environment Domain Risks by Stage of Information System Lifecycle** | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| **Information Governance** | | | |
| Adopt a Strategic Perspective on Information Integrity | Problems with "tone at the top" – the priority that business management places on addressing information integrity<br><br>Failure to include information integrity as part of the enterprise strategy<br><br>Failure to define responsibility and accountability for the enterprise's information assets<br><br>Missing or ineffective information integrity policies and standards<br><br>Failure to align information integrity requirements with business decision-making requirements | Failure to meet information users' needs consistently | Failure to adapt information governance to changes in business strategy |
| Address Human Resource Issues and Barriers to Implementing Information Integrity | Problems with "tone at the top" – the priority that business management places on addressing information integrity through organizational design, learning and innovation, etc.<br><br>Inappropriate benchmarks, scorecards and incentives<br><br>Failure to remove cultural and | Inconsistent communications<br><br>"Ill-health" of the socio-political environment. | Failure to manage impact of organizational change on information integrity |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | technology barriers to information integrity | | |
| Implement Information Integrity Program(s) | Failure to define information integrity priorities<br><br>Insufficient anticipation of malicious attacks, natural or environmental disasters<br><br>Problems with "tone at the top" – the priority that business management places on following good design, development and deployment practices (i.e., deliberately maintain a system with weaknesses to permit executive override)<br><br>Unsuitable governance, structures, processes, technology, policies, standards, etc.<br><br>Problems with quality of the physical IT environment and infrastructure and key system components | Performance expectations too low<br><br>Historically high failure experience<br><br>High visibility of failures, errors, problems, issues, etc.<br><br>Failure to enforce information integrity management practices. | Frequent environmental, regulatory, organizational (merger, downsizing, etc.), procedural changes<br><br>Frequent system changes of significant size<br><br>Large number of changes to the infrastructure<br><br>Large number of business units and processes affected<br><br>Difficulty of organizational change (low cultural tolerance/ low acceptance of change) |
| Prioritize Action Plans Based on Risk Assessment | Undefined risk assessment framework<br><br>Unaligned information integrity risks with business strategy<br><br>Unaligned information integrity risk | Inadequate resources for risk assessment<br><br>Incomplete risk identification and assessment<br><br>Executive override of priorities established | Failure to adapt risk management to changes in the business environment, organization and business operations. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | framework with business risk framework<br><br>No inventory of information integrity projects<br><br>Information integrity requirements not fully understood<br><br>Ineffective risk assessment and prioritization process<br><br>Low integration of information integrity in IT portfolio management system, etc. | through risk assessment<br><br>Failure to manage risk management process. | |
| Monitor Information Integrity and Implement Required Changes in Governance | Problems with “tone at the top” – the priority that business management places on change and change management.<br><br>Information Governance learning objectives are not defined<br><br>No inventory of information integrity controls<br><br>Monitoring redundancies and gaps exist between information governance and other related departments | Failure to monitor information governance process and obtain feedback. | Failure to adapt information quality management to changes in business and IT strategy, IT portfolio and information environment.<br><br>Failure to adapt monitoring, learning and change management to changes in Information Governance. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| **Definition, Design, Development, Deployment to Achieve Fit-for-Purpose -** | | | |
| Adopt a System Development Life Cycle (SDLC) at a Suitable Level of Maturity/Quality | User requirements omitted or misunderstood<br>Incompatible functions not identified<br>Lack of project management policies, standards and expertise<br>Information screens; outputs; ad hoc retrieval<br>User requirements incorrectly implemented<br>Untested/ code<br>Combination of incompatible functions<br>Fraudulent code | Failure to involve users; incomplete acceptance testing; no post-implementation review | Failure to adapt SDLC to changes in information requirements. For example, business intelligence requirements. |
| Establish Project Management Practices | Project management standards not defined.<br>Project management is not formalized (i.e. ad hoc) | Documentation is not maintained during the life of the project<br>External consultants are relied on to make business strategy related decisions | Failure to adapt project management to changes in information requirements. For example, system integration projects. |
| Identify Information Requirements | Information capture, transformation, aggregation and granularity not specified. | Users are not involved in the requirements analysis<br>Technology (i.e. leading edge) drives | Failure to modify requirements to reflect changes in information. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | | requirements instead of business use | |
| Acquire and/or Develop Process Components | Management has no guidance as to when it is appropriate to acquire and when it is appropriate to develop the solution internally<br><br>Process for identifying products, services and vendors not defined.<br><br>Combining disparate elements to produce required information. | Onerous RFI/RFP process limits pool of potential vendors<br><br>Management gets bogged down in RFI/RFP process | Failure to modify acquisition and development practices to adapt to changes in the type of information required. |
| Implement Process to Produce Information | Acceptance testing process not defined.<br><br>Post-implementation review not defined.<br><br>No guidance on when to back out of an implementation.<br><br>Conversion and import from other systems.<br><br>Implementation process does not require the ability to back out of a change. | No approval process for implementation<br><br>Cutover is not supervised by sufficiently senior staff.<br><br>Inadequate segregation of duties during the cutover.<br><br>Implementation is not sufficiently tested before changeover. | Failure to modify implementation practices to accommodate changes in how systems are developed. |
| Maintain System and Manage Change | Phases of maintenance, change request approvals, testing requirements, information quality framework not defined.<br><br>Lack of:<br><br>• Risk assessment | Failure to obtain approvals<br><br>Failure to test | Failure to adapt system maintenance and change management to changes in the environment, organization, business processes and system development practices. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | • Testing procedures<br>• Maintenance environment<br>• Emergency procedures | | |
| Manage User Development of Applications | Information integrity requirements of other users not identified.<br>Effective design standards not implemented. | Erroneous design of spreadsheets. data bases, etc. | Failure to reconfigure or modify user developed applications to account for changes brought about by changes in information systems. |
| Monitor SDLC Quality, Identify Required Changes and Manage Change Process | Learning objectives for quality assurance are not defined.<br>Quality assurance does not address secure design principles. | Errors after the system goes live are not monitored and prevents improvement of SDLC process | Failure to adapt SDLC to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| **Security – Access control, segregation of incompatible functions and asset safeguarding** | | | |
| Establish Responsibility and Accountability for Security | Authority, responsibility and accountability chain from Board to CEO to CIO, CSO and CISO not defined.<br>Internal audit's role not defined.<br>No advisory committee set up.<br>Responsibilities are not clearly defined<br>Accountability is not assigned to a single individual<br>Failure to document and communicate key responsibilities and accountabilities.<br>Budget inadequate<br>Non-disclosure agreements are not mandatory.<br>Inappropriate design of incident reporting and escalation rules.<br>Service level agreements for security not used | No follow-up to ensure responsibilities and accountabilities are understood | Failure to adapt security responsibilities/ accountabilities to changes in the environment, organization and business process. |
| Establish Environment and System Boundary Protections | Failure to define system boundary and zones within the boundary (external | Intrusion prevention/ detection fails. | Failure to adapt definition of system and zone boundaries to changes in the |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | public zone, external business zone, demilitarized zone, private internal high security zone).<br><br>Roles of users, owners, service providers not defined.<br><br>Errors in configuration of firewalls/intrusion prevention/detection.<br><br>Use of remote access, telecommuting not restricted.<br><br>Mobile computing practices not documented. | Virus/spyware protection fails.<br><br>Risks to the environment not identified or understood<br><br>Protection mechanisms not operated or maintained | environment, organization and business process. |
| Classify Information Assets According to their Sensitivity/Value | Failure to define scheme for classifying information assets according to their criticality and sensitivity.<br><br>No inventory of information assets. | Failure to classify all assets.<br><br>Information classification not current<br><br>Failure to track information on mobile devices. | Failure to adapt asset classification process to changes in the environment, organization and business process. |
| Assess Risks | Failure to define a risk assessment process that identifies threats and consequences.<br><br>Failure to separate common from infrequent but high consequence risks. | Failure to perform risk assessment for all units/processes and central. | Failure to adapt risk assessment process to changes in the environment, organization and business process. |
| Establish Security Policies, Standards and Guidelines to Address Risks | Policies to link management's objectives and operational procedures | Policies, standards and guidelines not enforced. | Failure to adapt security policies, standards and guidelines to changes in the environment, |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | insufficiently comprehensive.<br><br>Incomplete set of policies, standards and guidelines.<br><br>Failure to address security program, oversight responsibilities, roles and responsibilities, risk assessment framework, privilege management framework. | | organization and business process. |
| Ensure Personnel Have Required Qualifications and are Trustworthy | Failure to define both technical and ethical screening criteria.<br><br>Failure to use different screening criteria for regular and security personnel.<br><br>Performance standards, incentives not defined.<br><br>Ineffective training program and supervision.<br><br>Ineffective incentives.<br><br>Omission of outsourced functions.<br><br>Bonding not used. | Insufficient funding/staffing.<br><br>Failure to screen.<br><br>Failure to follow termination procedures.<br><br>Morale poor. | Failure to adapt hiring/termination procedures to changes in the environment, organization and business process. |
| Implement Information and Communication Program to Raise Security Awareness | Requirements of security awareness program do not take into account the nature of the internal and external users; employees, | Failure to execute communication awareness program or program too limited. | Failure to adapt communication program to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | contractors, outsourcers.<br>Design of security awareness program is ineffective. | | |
| Analyze User Access Requirements and Manage Privileges | Failure to define incompatible functions/roles.<br>Failure to define privileges by role.<br>Access permission lists and tables not based on principle of least privilege. | Failure to restrict privileges that enable users to tamper with information | Failure to adapt access privileges to changes in the environment, organization and business process. |
| Implement Physical Access Controls | Failure to include: both online and offline devices and media;<br>Design of physical access protection fails to employ a comprehensive set of access restriction techniques such as: Isolation, Hardening, Barriers,<br>Perimeter Surveillance, Keys, Access cards, and Biometric devices. | Unauthorised personnel can gain access to physical devices | Failure to adapt physical access controls to changes in the environment, organization and business process. |
| Implement Logical Access Management Techniques and Segregation of Incompatible Functions | Access requirements and restrictions not defined.<br>Appropriate logical access management techniques not used (i.e., Password, Card, Biometric) | Users with incompatible functions have access to data<br>Access overrides routinely given | Failure to adapt logical access management techniques to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| Manage Operations and Monitor Vulnerabilities | Failure to identify vulnerabilities for all critical components.<br>Failure to define intrusion prevention/detection process and incident response.<br>Ineffective intrusion prevention/detection.<br>Poor system component quality.<br>Failure to design crisis management procedures. | Incident response behaviour inadequate.<br>Failure to monitor vulnerability of security.<br>Failure to identify or report incidents. | Failure to adapt operations to changes in the environment, organization and business process. |
| Verify Procedural Compliance | Frequency and scope of procedural compliance verification (PCV) insufficient.<br>Tools for PCV inadequate.<br>Failure to co-ordinate with security administration.<br>Audit trails insufficient to enable PCV. | Failure to maintain logs, records, audit trails.<br>Failure to verify compliance with security procedures. | Failure to adapt compliance verification to changes in the environment, organization and business process. |
| Monitor Non-Compliance and Take Appropriate Remedial Action | Events to be logged and monitored not identified systematically.<br>Metrics not defined.<br>Security information management system not used. | Failure of security monitoring program. | Failure to adapt monitoring of security program to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| **Availability** | | | |
| Establish Responsibility and Accountability for Availability/Accessibility | Roles and responsibilities for planning and execution not defined.<br>No organization chart.<br>No procedure manual. | Failure to maintain responsibility and accountability | Failure to adapt responsibility/account ability for availability to changes in the environment, organization and business process. |
| Implement IT Environment Management Techniques | Access, processing and response time requirements for normal and crisis conditions not defined.<br>Routine maintenance procedures not documented. | Failure to maintain IT environment | Failure to adapt IT environment to changes in the environment, organization and business process. |
| Perform Routine Back-up & Recovery | Minor vs. Major recovery event not defined.<br>Procedures for handling minor disruptions not documented. | Failure to maintain routine back-up and recovery | Failure to adapt routine back-up and recovery to changes in the environment, organization and business process. |
| Plan for System Continuity | Onsite vs. Offsite issues not addressed in system continuity plan (SCP)<br>Onsite and Offsite system continuity procedures not developed. | Failure to maintain system continuity | Failure to adapt SCP to changes in the environment, organization and business process. |
| Monitor Information Availability Statistics and Make Required Changes | Failure to define availability metrics<br>Systems are not designed to alert users regarding | Failure to manage availability<br>Availability metrics/ trends are not monitored or reviewed. | Failure to adapt monitoring of availability to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | availability issues in a timely manner | | |
| **Dependability** | | | |
| Plan Capacity and Acquire and/or Develop Infrastructure | Capacity requirements not anticipated.<br>Network capacity too limited<br>Network capacity not related to risk assessment | Capacity overload | Failure to adapt capacity planning and infrastructure to changes in the environment, organization and business process. |
| Implement Service Level Agreements | Performance metrics and incentives not included in service level agreements (SLA).<br>SLA performance reporting not developed. | Non-compliance with SLA | Failure to adapt SLA to changes in the environment, organization and business process. |
| Implement Operations Procedures | Sequencing and scheduling not defined with information integrity perspective<br>Operational design sacrifices dependability for other objectives | In-house systems<br>• Size/capacity of facility Volume of processing<br>• Platform variety, size, etc.<br>• Age and maintenance of the facility; operational maturity; structural stability<br>• Location of the facility – proximity to local hazard(s); natural disasters<br>• Reliability of local infrastructure | Failure to adapt operations to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | | services – power, communications, civic services<br>• Local economic conditions<br>• Processing fluctuation, duration, or change<br>• Length of service of employees<br>• Type of employment arrangements – employee vs contractor<br>• Demands of the job<br>• Training and education<br>• Socio-political environment<br>• Culture<br>• Morale<br>Outsourced systems and services<br>• Nature of outsourced services provided<br>• Qualities of the service provider<br>• Ability to deliver<br>• Stability and size of the third party service provider<br>• Experience of the third party service provider | |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | | • History of service and performance<br>• Location of the third party service provider<br>• Regulations that relate to the outsourcing arrangement<br>• Quality of governance over third party service provider<br>• Quality of the contract – clarity of roles and responsibilities, statement of work, service levels, etc.<br>• Relationship between the entity and the third party service provider | |
| Manage Configuration and Version Management | Configuration requirements and version management not anticipated<br>Ineffective configuration and version management procedures | Configuration errors.<br>Failure to manage versions. | Failure to adapt configuration to changes in the environment, organization and business process. |
| Monitor Dependability of Information Processing and Make Required Changes | Failure to define predictability and dependability metrics<br>Ineffective operations monitoring procedures | Failure to monitor program stability | Failure to adapt monitoring of dependability of operations to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| **Consistency** | | | |
| Establish Standards | Failure to define standards across the enterprise.<br>Failure to design integration process to enable consistency and comparability. | Incomplete implementation of standards. | Failure to adapt standards to changes in the environment, organization and business process. |
| Verify Compliance with Standards | Failure to define compliance with the policies and procedures that affect information integrity.<br>Ineffective compliance verification program.<br>Restricted scope. | Ineffective compliance verification. | Failure to adapt compliance verification to changes in the environment, organization and business process. |
| Monitor Non-Compliance and Take Remedial Action | Consistency/ comparability monitoring metrics not defined.<br>Maintaining consistency/ comparability is not explicit design objective | Ineffective monitoring of consistency/comparability. | Failure to adapt monitoring of consistency to changes in the environment, organization and business process. |
| **Verifiability** | | | |
| Establish Audit Trails | Failure to consider elements of the audit trail that depend on manual and automated, visible and invisible, cross references and process documentation.<br>Failure to incorporate audit trail | Failure to capture all elements required to create an audit trail from source to final disposition. | Failure to adapt audit trail to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | requirements into the design of business process components. | | |
| Establish Data/Information Retention and Disposal Policies | Retention/disposal policies inconsistent with verifiability/auditability objectives.<br>Metadata not used to document retention/disposal requirements. | Failure to retain information for subsequent follow up or verification. | Failure to adapt information retention to changes in the environment, organization and business process. |
| Acquire Audit Tools | CAATS and other analysis tools not available to support verifiability/auditability objectives.<br>Logging tools not used.<br>Scanning/extraction tools not used.<br>Analysis/reporting tools not used. | Audit tools are not secured from unauthorized access.<br>Production data used in conjunction with audit tools is not secured. | Failure to adapt audit tools to changes in the environment, organization and business process. |
| Monitor Identified Gaps and Implement Changes to Eliminate Those Gaps | Information integrity monitoring and learning objectives for audit personnel are not defined.<br>Audits are not effectively integrated between departments (e.g. security, internal audit, external audit, etc.). | Users rare not trained to use audit tools<br>Lack of effective use of audit tools prevents the effective monitoring of risks. | Failure to adapt monitoring of verifiability to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| **Assurance** | | | |
| Implement an Information Integrity Assurance Program | Objectives of information integrity assurance program not defined.<br><br>Objectives of information integrity assurance program too limited (e.g., omit information integrity policies, risk assessment process, etc.).<br><br>Information integrity assurance program not developed. | Failure to achieve repeatable/sustainable level of maturity in information integrity assurance program. | Failure to adapt information integrity assurance program to changes in the environment, organization and business process. |
| Have Internal Audit Provide Periodic Assurance on Information Integrity | Respective areas of responsibility not defined for financial auditing, compliance auditing, operational auditing, IT auditing.<br><br>Lack of co-ordination between audit groups with overlapping but distinct responsibilities.<br><br>Failure to integrate information integrity objectives effectively into operational audits.<br><br>Scope of audits too restricted. | Non-sampling and sampling risk. | Failure to adapt internal audit priorities to changes in the environment, organization and business process. |
| Have External Audit Provide Periodic Assurance on Information Integrity | Litigation concerns limit scope of audit.<br><br>Financial audit perspective may not | Non-sampling and sampling risk. | Failure to adapt external audit priorities to changes in the environment, organization and business process. |

| | Illustrative Environment Domain Risks by Stage of Information System Lifecycle | | |
|---|---|---|---|
| **Activity** | **Creation** | **Operation** | **Change** |
| | afford broad enough design of audit.<br>Materiality may be too big. | | |
| Monitor Information Integrity Assurance Outcomes, Learn From Them and Implement Required Changes | Failure to monitor credibility-adding process.<br>Failure to design compliance procedures to address standards. | Failure to follow standards. | Failure to remediate processes with identified information integrity problems.<br>Failure to adapt monitoring process to changes in the environment, organization, technology and business process. |

## *Summary*

Up to this point in this publication, three domains of risks, enablers and controls have been identified: the content domain, the process domain and the IS environment domain. Recall that the onionskin model presented in the introduction portrays an IS environment domain that surrounds and envelops the process domain and content domains. The process domain, in turn, envelops most of the content domain. (Some aspects of metadata such as user understanding of the nature and purpose of certain data and information may exist outside the process domain and are therefore not entirely enveloped by it.)

The next three chapters discuss enablers and controls that can address the risks identified in the previous three chapters and help ensure the integrity of information. Working from the outside layers of the onionskin model, Chapter 6 covers the IS environment domain, Chapter 7 covers the process domain and Chapter 8 covers the content domain.