| **IT Risk Scenario: Unauthorized Access of Information** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | Sensitive information is accessed or viewed by unauthorized persons due to inadequate quality or protection practices for storage, retention, archiving or disposing of information | | |
| **Risk Type** | 3-Data and system protection; 4-Legal and regulatory | | |
| **Risk Scenario Category** | Data and information management: Inability to achieve and preserve adequate data and information quality and protection | | |
| **Risk Scenario Reference** | 18A | | |
| **Risk Statement** | Unauthorized disclosure of sensitive information through email or social media occurs resulting in press attention, legal and regulatory actions, or theft of intellectual property. | | |
| **Risk Owner** | CIO/CTO/Data or Privacy Officer | **Risk Oversight** | I&T Steering Board  Operational Risk Management |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Nonmalicious Insider | | |
| **Intent/ Motivation** | Inadvertent disclosure | | |
| **Threat Event** | Sensitive information is not properly stored, archived or marked with appropriate classification. | | |
| **Assets/Resources** | Sensitive, nonpublic, or proprietary information and data | | |
| **Consequence** | Sensitive, nonpublic information and data are viewed by unauthorized persons. | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | Poor data and information management leads to decreased productivity, rework, and time spent on locating needed information. |
| * Cost of Response | Cost associated with implementing corrective measures including legal fees, fines, external communications, etc. |
| * Replacement Cost | N/A |
| * Competitive Advantage | Loss or theft of intellectual property or other data types may impact new or existing product and services delivery. |
| * Reputation | Internal weaknesses discovered by the public may impact customer perception and lead to trust violations. |
| * Fines and Judgements | Violation of customer privacy regulations may lead to fines. |
| **Timing** | This risk requires ongoing management of data and information over the life cycle of the assets. If there are repeated audit findings on data quality, storage, retention, archival and disposal, corrective action should be prioritized and made an ongoing part of daily work. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | Exposure to data loss results in continued press attention, legal and regulatory actions, or theft of intellectual property, firing of key staff, and reputation damages. Key staff leave the organization resulting in loss of institutional knowledge that slows the cleanup/repair efforts. |
| **Typical or Most Likely Case** | Several recurring information and data leakage and inadvertent access incidents happen over a period of several months to years. Audit findings repeatedly expose issues before action is taken to improve data and information quality, retention, storage, management and disposal. |
| **Best Case** | The incident is a one-time event and is found quickly. Data clean up, life cycle management, and classification procedures are established and maintained. |
| **Assumptions** | * Information was released from inside the business through an official channel of communication inadvertently. * Access controls for information and data are out of alignment with the access needed for the role. * Information is not treated as a critical asset of the organization. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **APO01.05 Establish roles and responsibilities.** Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability. | Management | Yes | No | Yes | COBIT APO01.05 |
| 2 | **APO01.07 Define information (data) and system ownership.**  Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification. | Management | Yes | Yes | Yes | COBIT APO01.07 |
| 3 | **APO14.01 Define and communicate the organization’s data management strategy and roles and responsibilities.**  Define how to manage and improve organization data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner. | Preventive | Yes | No | Yes | COBIT APO14.01 |
| 4 | **APO14.04 Define a data quality strategy.**  Define an integrated, organization-wide strategy to achieve and maintain the level of data quality (such as complexity, integrity, accuracy, completeness, validity, traceability and timeliness) required to support the business goals and objectives. | Preventive | Yes | No | Yes | COBIT APO14.04 |
| 5 | **APO14.08 Manage the life cycle of data assets.** Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement. | Preventive | Yes | Yes | Yes | COBIT APO14.08 |
| 6 | **BAI09.03 Manage the asset life cycle.**  Manage [information and data] assets from procurement to disposal. Ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired. | Management | Yes | Yes | Yes | COBIT BAI09.03 |

|  |  |  |  |
| --- | --- | --- | --- |
| **E. Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Data and information roles & responsibilities | Number of I&T-related roles assigned to individuals | Lead |
| 2 | Data and information roles & responsibilities | Percent of data assets with clearly defined owners | Lead |
| 3 | Data and information roles & responsibilities | Percent of information systems with clearly defined owners | Lead |
| 4 | Data and information management | Percent of information items classified according to the agreed classification levels | Lead |
| 5 | Data and information management | Percent of data subject to a categorization/classification scheme  Number of data management breaches or unauthorized/inadvertent access in comparison to the defined strategy | Lag |
| 6 | Data and information management | Percent of stakeholders satisfied with the quality of data | Lag |
| 7 | Data and information management | Number of requirements from data consumers that cannot be mapped to a data source | Lag |
| 8 | Data and information management | Percent of assets managed from procurement to disposal | Lag |
| 9 | Data and information management | Percentage of assets deployed following the standard implementation life cycle | Lag |