| **IT Risk Scenario: Security Configuration Intentionally Modified** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | The security configuration is intentionally modiﬁed or manipulated | | |
| **Risk Type** | 2-Service quality; 3-Data and system protection; 5-Workplace safety | | |
| **Risk Scenario Category** | User access rights management: Inability to protect systems from malicious or inadvertent system compromise, misuse or loss | | |
| **Risk Scenario Reference** | 7C | | |
| **Risk Statement** | Authorized users with access to information resources intentionally modify the asset configuration, maliciously affecting the confidentiality, integrity or availability of systems | | |
| **Risk Owner** | CIO/CTO/CDO/CISO | **Risk Oversight** | Chief Risk Officer (CRO) |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Malicious insiders | | |
| **Intent/ Motivation** | Authorized users with access to information resources intentionally affect the confidentiality, integrity or availability of systems, causing a security incident. | | |
| **Threat Event** | A security incident is caused by the actions of an insider. | | |
| **Assets/Resources** | Entire IT operation systems | | |
| **Consequence** | Security incidents, including data disclosure, tampering and outages | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | System unavailability or lack of data integrity can affect the productivity of the entire organization. |
| * Cost of Response | Time/efforts to identify root causes and recover from an incident |
| * Replacement Cost | N/A |
| * Competitive Advantage | If the events(s) are severe enough and public-facing, the organization can lose customers and a competitive advantage. |
| * Reputation | If the events(s) are severe enough and public-facing, organization reputation can be adversely impacted due to nonavailability and delays. |
| * Fines and Judgements | If the events(s) are severe enough and public-facing, exposure to fines and regulatory and legal compliances is possible. |
| **Timing** | * The duration of the incident can be very short or prolonged, depending on job scope and overlap of duties. * Early detection and corrective action are *key* to limit the scope and nature of this risk scenario. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | Security and outage incidents can result in mass outages, reportable data breaches, a loss of competitive advantage, and fines and judgements. Staff are fired, morale is low and costs to clean up increase over time. |
| **Typical or Most Likely Case** | The scope and size of incidents and outages are limited and responded to without lasting damage to the organization. |
| **Best Case** | Limited features/functions of systems are affected, quickly recovered and corrective employee action is immediately taken. |
| **Assumptions** | * Data and systems are effectively backed up and available for immediate restore if required. * Standard operating procedures and change management process are in place * Policy and procedures documentation is available. * Software test and release procedures are in place. * Disaster recovery plan and procedure are in place and up to date. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **APO01.02 Communicate management objectives, direction and decisions made.**  Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization. | Preventive | Yes | No | Yes | COBIT APO01.02 |
| 2 | **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 | Yes | Yes | COBIT APO14.04 |
| 3 | **BAI03.05 Build solutions.**  Install and configure solutions and integrate with business process activities. During configuration and integration of hardware and infrastructure software, implement control, security, privacy and auditability measures to protect resources and ensure availability and data integrity. Update the product or services catalogue to reflect the new solutions. | Preventive | Yes | Yes | Yes | COBIT BAI03.05 |
| 4 | **DSS05.01 Protect against malicious software.**  Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam). | Preventive | Yes | Yes | Yes | COBIT DSS05.01 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Program & quality management | Frequency of communication on management objectives and direction for I&T | Lead |
| 2 | Program & quality management | Number of data quality improvement efforts identified and recorded in a sequence plan | Lead |
| 3 | Program & quality management | Percent of employees failing tests on malicious attacks (e.g., test of phishing email) | Lag |
| 4 | Data & information management | Number of successful malicious software incidents | Lag |
| 5 | Solution requirements & design | Number of software problems reported | Lead |
| 6 | Solution requirements & design | Number of software review errors | Lead |