| **IT Risk Scenario: IT Services Change Management** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | IT services change management is inadequate to meet service delivery requirements | | |
| **Risk Type** | 2-Service quality; 6-Product & service cost | | |
| **Risk Scenario Category** | IT cost and oversight: Inability to provide IT services within agreed-on and reasonable resource limitations | | |
| **Risk Scenario Reference** | 3B | | |
| **Risk Statement** | Inadequate change management leads to service delivery failures, inability to meet user needs and increased costs due to rework. | | |
| **Risk Owner** | Business Process Owner/CIO/CTO/CDO | **Risk Oversight** | I&T Governance Board  Steering Committee (programs/projects) |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Enterprise insider(s), partners or vendors | | |
| **Intent/Motivation** | The business wants the solutions to be implemented without delay to improve processes or does not have the organizational maturity to implement adequate change processes. | | |
| **Threat Event** | The risk scenario may be intentionally, but not maliciously, caused.  Threat events include:   * Inadequate change management knowledge and experience lead to insufficient quality controls prior to release of a solution. Substandard solutions result in incorrect computing results and business decisions. * An untrained insider or a trained insider may not detect incorrect computing results. | | |
| **Assets/Resources** | * Employee productivity is affected by system deficiencies, and inaccurate and unreliable services. * The confidentiality, integrity and availability of any system or information are at risk due to poor change control. | | |
| **Consequence** | Incorrect computing results and business decisions can cause financial loss, reputational damage, regulatory implications and competitive disadvantage | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | * Inefficient products, and long maintenance and business decision implementation cycle have a negative impact on the productivity in the business * Inefficient use of financial resources, employees, contract workers and consultants |
| * Cost of Response | Rework and incident response impact costs |
| * Replacement Cost | N/A |
| * Competitive Advantage | The benefits of new products and services may not be realized due to delays in delivery |
| * Reputation | Adverse impact on image and reputation of organization due to inefficient products and services |
| * Fines and Judgements | N/A |
| **Timing** | * The duration from the introduction of the poor service delivery solutions until incorrect computing results are detected can be very short or prolonged * Inadequate change control may take place based on gaps in functionality and may appear in an ad-hoc manner * The time lagcan be short or long, depending on the nature of the monitoring, detection and type of risk materialized | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | Continued rework and associated costs to clean up the rework continue for a long period of time and no effort is made to correct them. This may result in staff burnout and continued service delivery interruptions that lead to a devastating outcome, e.g., reputational damage, financial loss, bankruptcy, loss of customer base, competitive disadvantage. Talent leaves the business, and it is not able to attract new talent. The board may intervene, and senior managers/decision makers are asked to leave the business. |
| **Typical or Most Likely Case** | The inadequate change control and associated misconfigurations that may be in production are detected, but the deviation from prior results determines how quickly the misconfiguration is detected. The business may be well into the decision process before the error is picked up. |
| **Best Case** | The inadequate change control processes are detected as soon as they are produced and well before the business gets to the point where it considers which decisions it needs to make. There are controls in place that pick up deviations from prior results. |
| **Assumptions** | * Ad-hoc changes are implemented regularly and not as exception. * Quality controls are not adequately observed. * The monitoring of implementation policies, procedures and rules are not completely communicated and understood by decision makers. * Lack of oversight and testing control over applications. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **EDM04.03 Effective resource management.**  Monitor the key goals and metrics of the resource management processes. Determine how deviations or problems will be identified, tracked and reported for remediation. | Detective | Yes | No | Yes | COBIT EDM04.03 |
| 2 | **BAI05.03 Communicate desired vision.**  Communicate the desired vision for the change in the language of those affected by it. The communication should be made by senior management and include the rationale for, and benefits of, the change; the impacts of not making the change; and the vision, the road map and the involvement required of the various stakeholders. | Preventive | Yes | Yes | Yes | COBIT BAI05.03 |
| 3 | **BAI06.01 Evaluate, prioritize and authorize change requests.**  Evaluate all requests for change to determine the impact on business processes and I&T services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled. | Preventive | Yes | Yes | Yes | COBIT BAI06.01 |
| 4 | **DSS02.03 Verify, approve and fulfill service requests.**  Select the appropriate request procedures and verify that the service requests fulfill defined request criteria. Obtain approval, if required, and fulfill the requests. | Detective | No | No | Yes | COBIT DSS02.03 |
| 5 | **DSS02.04 Investigate, diagnose and allocate incidents.**  Identify and record incident symptoms, determine possible causes, and allocate for resolution. | Detective | No | No | Yes | COBIT DSS02.04 |
| 6 | **DSS03.02 Investigate and diagnose problems.** Investigate and diagnose problems using relevant subject matter experts to assess and analyze root causes. | Detective | No | No | Yes | COBIT DSS03.02 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Program/project monitoring | Number of benefits (e.g., cost savings) achieved through optimum utilization of resources | Lag |
| 2 | Program/project monitoring | Number of resource management performance targets realized | Lag |
| 3 | Stakeholder engagement | Level of stakeholder feedback on resource optimization  Number of questions regarding the change | Lead |
| 4 | Stakeholder engagement | Stakeholder feedback on level of understanding of the change | Lead |
| 5 | Business impact due to change | Amount of rework caused by failed changes | Lag |
| 6 | Business impact due to change | Percentage of unsuccessful changes due to inadequate impact assessments | Lag |
| 7 | Service desk incidents due to change | Mean elapsed time for handling each type of service request | Lag |
| 8 | Service desk incidents due to change | Number of identified and recorded incident symptoms  Number of correctly determined symptom causes | Lag |
| 9 | Service desk incidents due to change | Number of duplicate problems in the reference log | Lag |