| **IT Risk Scenario: Third-Party Suppliers** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | Third-party suppliers do not deliver projects as per contractual agreements (any combination of exceeded budgets, quality problems, missing functionality, late delivery) | | |
| **Risk Type** | 1-Product delivery; 2-Service quality | | |
| **Risk Scenario Category** | Third-party supplier incidents: Inability to meet service level requirements because of failure of third-party suppliers | | |
| **Risk Scenario Reference** | 11C | | |
| **Risk Statement** | Delays in software ﬁxes to the online retail website occur due to software vendors who fail to meet requirements for timeliness and quality. | | |
| **Risk Owner** | Portfolio Manager/CIO/CTO/CDO | **Risk Oversight** | IT Governance Board  Architecture Board  Steering Committee (Programs/  Projects)  Chief Risk Officer (CRO) |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Untrained/accidental insiders | | |
| **Intent/ Motivation** | Inadvertent, nonmalicious | | |
| **Threat Event** | The event is unlikely to occur in a single event but can occur through a series of decision-making processes (portfolio and program/project governance) that are undertaken because of inaccurate or incomplete information. | | |
| **Assets/Resources** | * Online retail website * Software that facilitate the operation of the online retail website | | |
| **Consequence** | Inability to serve customers through an online website | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | By compromising the operations of the website, the economic or customer service provided by the enterprise online presence can be stopped. |
| * Cost of Response | Incomplete delivery generates the need for further phases or additional project to deliver the complete required outcomes. |
| * Replacement Cost | N/A |
| * Competitive Advantage | The delay in the business process and I&T operations supported by the service provider can be used by competitors to gain an advantage. |
| * Reputation | N/A |
| * Fines and Judgements | N/A |
| **Timing** | * Early **detection** of the service provider failures and **corrective actions** are imperative to minimize impact. * The **time lag** between an issue surfacing and being addressed can be short or long, depending on the frequency and effectiveness of program and project status reporting and vendor management. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | The website stops operating because its software fixes are not received in time and its operation cannot proceed without these critical fixes. The enterprise loses customers because agreed-on service levels are not achieved. The critical IT providers can eventually be replaced, but it will take months to switch to different providers. Customers bring legal actions against the enterprise because it did not meet the agreed-on level of service. |
| **Typical or Most Likely Case** | The website operates but customers experience some errors, which increases the number of calls to the service center due to customer complaints. This results in high demand for customer service agents to handle complaints. The enterprise loses only a few customers, and the service provider improves its service delivery or can be replaced in a timely manner. |
| **Best Case** | The website continues to operate, and customers experience only a slow response level in its operation. |
| **Assumptions** | * The website depends on the third-party service provider because the enterprise has no expertise inside its organization. * The enterprise has an established contract with the software provider that includes the expected service levels in software fixes. * The enterprise has many of its business processes supported by this software provider. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **APO06.03 Create and maintain budgets.**  Prepare a budget reflecting investment priorities based on the portfolio of I&T enabled programs and I&T services. | Preventive | Yes | Yes | Yes | COBIT APO06.03 |
| 2 | **APO07.01 Acquire and maintain adequate and appropriate staffing.**  Evaluate internal and external staffing requirements on a regular basis or upon major changes to the enterprise, or operational or IT environments, to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. | Preventive | Yes | Yes | Yes | COBIT APO07.01 |
| 3 | **APO07.06 Manage contract staff.**  Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with organization policies and meet agreed-on contractual requirements. | Preventive | Yes | Yes | Yes | COBIT APO07.06 |
| 4 | **APO09.03 Define and prepare service agreements.**  Define and prepare service agreements based on options in the service catalogs. Include internal operational agreements. | Preventive | Yes | Yes | Yes | COBIT APO09.03 |
| 5 | **APO09.05 Review service agreements and contracts.**  Conduct periodic reviews of the service agreements and revise when needed. | Preventive | Yes | Yes | Yes | COBIT APO09.05 |
| 6 | **APO10.01 Identify and evaluate vendor relationships and contracts.**  Continuously search for and identify vendors, and categorize them into type, significance and criticality. Establish criteria to evaluate vendors and contracts. Review the overall portfolio of existing and alternative vendors and contracts. | Preventive | Yes | Yes | Yes | COBITAPO10.01 |
| 7 | **APO10.03 Manage vendor relationships and contracts.**  Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes. | Preventive | Yes | Yes | Yes | COBIT APO10.03 |
| 8 | **BAI04.02 Assess business impact.**  Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA). | Preventive | Yes | Yes | Yes | COBIT BAI04.02 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Resource & budget planning | Number of identified shortfalls and missing skills in planning for staffing | Lead |
| 2 | Resource & budget planning | Frequency of periodic reviews conducted to ensure correctness and compliance of contractor’s staff | Lead |
| 3 | Vendor risk management | Number of scenarios created to assess future availability situations | Lead |
| 4 | Vendor risk management | Percentage of business process owners signing off on analysis results | Lead |
| 5 | Vendor risk management | Percentage of defined evaluation criteria achieved for existing suppliers and contracts | Lead |
| 6 | Vendor risk management | Percentage of alternative suppliers providing equivalent services of existing supplier contracts | Lead |
| 7 | Vendor risk management | Number of business processes with undefined service agreements | Lead |
| 8 | Vendor risk management | Percentage of live IT services covered by service agreements | Lead |