| **IT Risk Scenario: Vendor Support Ends** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | Vendor support comes to an end for an I&T component | | |
| **Risk Type** | 1-Product delivery; 2-Service quality; 6-Product & service cost | | |
| **Risk Scenario Category** | IT hardware: Inability to continually support and maintain technology systems (including aging and legacy systems) that are supporting business processes | | |
| **Risk Scenario Reference** | 9M | | |
| **Risk Statement** | The vendor of a legacy system used by the enterprise has ceased all support for the system, resulting in total service interruption in case of a hardware defect or systems failure. | | |
| **Risk Owner** | Portfolio Manager/CIO/CTO/CDO | **Risk Oversight** | I&T Governance Board  Architecture Board  Steering Committee (Programs/ Projects)  Chief Risk Officer (CRO) |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Threat actor may be the third-party supplier, if vendor support has been terminated without adequate warning notice. If notice was supplied, the actors are insiders if there was awareness and no action taken. | | |
| **Intent/ Motivation** | Intent is inadvertent. | | |
| **Threat Event** | The threat event occurs at the point when service support for the system ends. At this point, it remains a business risk, and there is no impact until a system malfunction occurs and cannot be rectified due to the lack of support. | | |
| **Assets/Resources** | The assets at risk are those business processes and activities that are enabled by the system that is no longer supported. | | |
| **Consequence** | Loss only occurs if a hardware defect or failure occurs; the lack of support does not in itself invoke a loss.Business processes and activities that are enabled by the system are no longer available if the hardware fails. | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | Business process is halted, impacting any dependent customer processes and users of the system can no longer complete their work and productivity is affected. |
| * Cost of Response | Root cause investigation needs to be completed to identify and validate the cause of the disruption to business process. Alternative business process must be developed, pending hardware replacement. |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | * Replacement Cost | Replacement systems need to be identified, procured and then tested prior to implementation. |
| * Competitive Advantage | If the system impacted is one which supports a business area or process where the business has a competitive advantage, then this may be disrupted or potentially lost completely if the incident cannot be correctly resolved. |
| * Reputation | Interruption of the specific business process may disrupt broader business activities, and business and customer processes with consequent adverse publicity and reputational impact. |
| * Fines and Judgements | Not applicable unless there is an extended outage period and the failed system supports critical business and/or regulatory processes. |
| **Timing** | * Service interruption may relate to critical business process with critical processing times and periods (end of month) where delays have greater impact. * Time taken to identify error, triage and identify alternate business process or fix issue may also impact business process key timings. * Any need to implement a replacement may result in business process disruption during period of procurement and testing, and also at the point of implementation. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | Hardware defect results in total system shutdown with no alternate IT or business resilience available, and business processes are unable to be completed. |
| **Typical or Most Likely Case** | Alternative business processes are planned that can be used to bypass the system in the event of hardware failure, but these are untested; hence, the overall resilience of the business processes is uncertain. Ad-hoc arrangements (service extensions) have been agreed on with vendor for limited additional service support. Alternate business processes are planned but not tested or launched. |
| **Best Case** | Alternate business processes are available and in use that can be used to bypass the system in the event of hardware failure, and there is a funded project to remove the system from the IT estate. |
| **Assumptions** | * The hardware component is no longer manufactured and cannot easily be replaced by an off-the-shelf purchase. * The hardware component is unable to be repaired or fixed, by either the original supplier or an alternate in-house or third-party supplier. * The business has not procured additional extended-life hardware service support through an arrangement with the original supplier or another qualified third party. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Controls to Mitigate the Risk Scenario** | | | | | | |
| **Control Description** | | **Control Type** | **Effect on Impact** | **Effect on Frequency** | **Essential Control** | **Reference** |
| 1 | **EDM02.01 Establish the target investment mix.**  Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree  of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary. | Preventive | No | Yes | Yes | COBIT EDM02.01 |
| 2 | **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 |
| 3 | **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 | COBIT APO10.01 |
| 4 | **APO10.04 Manage vendor risk.**  Identify and manage risk relating to vendors’ ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor. | Preventive | Yes | Yes | Yes | COBIT APO10.04 |
| 5 | **BAI04.01 Assess current availability, performance and capacity, and create a baseline.**  Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against service-level agreements (SLAs). Create availability, performance and capacity baselines for future comparison. | Preventive | Yes | Yes | Yes | COBIT BAI04.01 |
| 6 | **BAI09.02 Manage critical assets.**  Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs. | Preventive | Yes | Yes | Yes | COBIT BAI09.02 |
| 7 | **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). | Preventative | Yes | Yes | Yes | COBIT BAI04.02 |
| 8 | **DSS04.02 Maintain business resilience.**  Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption. | Preventive | Yes | Yes | Yes | COBIT DSS04.02 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Service capacity & availability planning | Percent of service targets being met | Lead |
| 2 | Service capacity & availability planning | Number of reviews of the service agreements performed | Lead |
| 3 | Service capacity & availability planning | Number of service agreements revised, as needed | Lead |
| 4 | Service capacity & availability planning | Percent of actual capacity usage | Lag |
| 5 | Service capacity & availability planning | Percent of actual availability | Lag |
| 6 | Service capacity & availability planning | Percent of actual performance | Lag |
| 7 | Business impact analysis | Number of scenarios created to assess future availability situations | Lead |
| 8 | Business impact analysis | Percent of business process owners signing off on analysis results | Lead |
| 9 | Business impact analysis | Percent of key stakeholders involved in business impact analyses evaluating the impact over time of a disruption to critical business functions and the effect that a disruption would have on them | Lead |