| **IT Risk Scenario: Failure to Implement Regulatory Changes** | | | |
| --- | --- | --- | --- |
| 1. **Risk Scenario Description** | | | |
| **Risk Scenario Title** | The enterprise is unaware of regulatory changes that have a business impact on the availability of critical workers | | |
| **Risk Type** | 1-Product delivery; 4-Legal & regulatory; 5-Workplace safety | | |
| **Risk Scenario Category** | Noncompliance: Inability to comply with policies, standards, laws and regulations related to technology | | |
| **Risk Scenario Reference** | 12B | | |
| **Risk Statement** | The enterprise does not implement changes to workplace health and safety regulations. | | |
| **Risk Owner** | Business Process Owner/CIO/CTO/CDO | **Risk Oversight** | Head of Human Resources  Head of Compliance  Chief Risk Officer |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Risk Scenario Components** | | | |
| **Actor/Threat Community** | Nonmalicious internal employees, contractors and consultants | | |
| **Intent/ Motivation** | The inadvertent event resulting from untrained staff, inadequate process/documentation, lack of understanding of the local and international regulations. | | |
| **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. * The event may also occur if pressure is exerted to commence activity before the requirements that comply with changes to regulations are fully clarified and defined. | | |
| **Assets/Resources** | Availability of staff, contractors, vendors, suppliers and consultants | | |
| **Consequence** | Unavailability of critical staff needed to continue to operate in a safe manner to deliver organizational products and services. | | |
| **Impact Dimensions (potential forms of loss)** | * Productivity | Impacts daily operating procedures (employees not able to perform business process). |
| * Cost of Response | * Operating cost increases to locate skilled resources. * System downtime causes enterprise to lose customers and stops employees from providing services. |
| * Replacement Cost | N/A |
| * Competitive Advantage | N/A |
| * Reputation | Negative perception and reputation damage result from a reputation for not regarding worker safety. |
| * Fines and Judgements | * Fines may be a factor in data breach scenarios (e.g., GDPR, CCPA, FTC). * Judgements and other lawsuits may be a factor in data breach scenarios. |
| **Timing** | * Inadequate analysis of regulations leads to unintended noncompliance and, a, incurred fines. * The **duration** of the incident can be very short or prolonged. * Early **detection** of the local/international laws and regulations is key to limiting the scope of the incident. * The **time lag** can be short or long, depending on the nature of the action taken by management. | | |

|  |  |  |
| --- | --- | --- |
| 1. **Risk Scenario Scope & Extent** | | |
| **Extent of the Scenario** | **Worst Case** | Serious workplace safety incident occurs, and people are hurt or killed. The incident has major damage to the brand/enterprise. High fines are levied on the enterprise for noncompliance with workplace safety regulations. Reputation is tarnished and additional regulatory scrutiny continues for several years. The cost of compliance is high and takes resources that can be used for other programs. It is difficult to attract and retain talent in the workforce. |
| **Typical or Most Likely Case** | No serious workplace safety incident occurs. The cost of compliance is high and takes resources that can be used for other programs. It is difficult to attract and retain talent in the workforce. |
| **Best Case** | Regulatory changes are simple and can be resolved before the situation results in a workplace safety incident. |
| **Assumptions** | * The organization has a defined compliance program and project management life cycle and methodology, either internal or an externally defined approach. * The defined methodology is fully implemented and adopted for the project/program. * The organization relies on its staff to monitor for changes to the environment but does not hire, train or upskill them properly to perform the role. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | Yes | Yes | COBIT APO01.02 |
| 2 | **APO01.09 Define and communicate policies and procedures.**  Put in place procedures to maintain compliance with, and performance measurement of, policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework. | Preventive | Yes | Yes | Yes | COBIT APO01.09 |
| 3 | **APO04.03 Monitor and scan the technology environment.**  Set up a technology watch process to perform systematic monitoring and scanning of the enterprise external environment to identify emerging technologies that have the potential to create value (e.g., by realizing the enterprise strategy, optimizing costs, avoiding obsolescence, and better enabling enterprise and I&T processes). Monitor the marketplace, competitive landscape, industry sectors, and legal and regulatory trends to be able to analyze emerging technologies or innovation ideas in the enterprise context. | Preventive | Yes | Yes | Yes | COBIT APO04.03 |
| 4 | **APO07.03 Maintain the skills and competencies of personnel.**  Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals. | Preventive | Yes | Yes | Yes | COBIT APO07.03 |
| 5 | **APO12.02 Analyze risk.**  Develop a substantiated view on actual I&T risk, in support of risk decisions. | Preventive | Yes | Yes | Yes | COBIT APO12.02 |
| 6 | **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 |
| 7 | **DSS01.05 Manage facilities.**  Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines. | Preventive | Yes | Yes | Yes | COBIT DSS01.05 |
| 8 | **MEA03.01 Identify external compliance requirements.**  On a continuous basis, monitor changes in local and international laws, regulations and other external requirements and identify mandates for compliance from an I&T perspective. | Preventive | Yes | Yes | Yes | COBIT MEA03.01 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Key Risk Indicators** | | | |
|  | **Indicator** | **KRI Description** | **Lead/Lag** |
| 1 | Policies and procedures | Percentage of active policies and procedures that are documented and up to date | Lead |
| 2 | I&T management communications | Frequency of communication on management objectives and direction for I&T | Lead |
| 3 | Human resources management | Number of training programs provided | Lead |
| 4 | Human resources management | Number of people trained on health and safety guidelines | Lead |
| 5 | Human resources management | Number of staff aware and able to demonstrate competency with respect to policies and procedures | Lead |
| 6 | Risk management | Number of risk scenarios defined for environmental threats | Lead |
| 7 | Risk management | Frequency of compliance requirements reviews | Lead |
| 8 | Risk management | Number of critical noncompliance issues identified per year | Lead |
| 9 | Risk management | Percentage of satisfaction of key stakeholders in regulatory review compliance process | Lead |