|  |
| --- |
| **Maturity Assessment Report for EDM01**  **Ensured Governance Framework Setting and Maintenance**  Organisation: NWU Assessment: COBIT 2019  Lead Assessor: John Smith Focus Area: General Code Model  Auditor: Alice Johnson Audit Name: Audit 1  Target Level: 4 Year: 2023  Maturity Level: 5 |

**Description:**

Analyse and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise’s mission, goals, and objectives.

**Purpose:**

Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise’s strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual, and regulatory requirements is confirmed; and the governance requirements for board members are met.

1. **Enterprise goal compliance (51%)**
   1. This governance objective supports the achievement of a set of primary enterprise goals and metrics:

* EG03 - Compliance with external laws and regulations

|  |  |  |
| --- | --- | --- |
| **Metric** | **Importance** | **Rating** |
| Number of regulatory noncompliance issues relating to contractual agreements with business partners | 8 | Largely Achieved |
| Number of regulatory noncompliance issues causing public comment or negative publicity | 4 | Partially Achieved |
| Cost of regulatory noncompliance, including settlements and fines | 3 | Partially Achieved |
| Number of noncompliance matters noted by regulators | 2 | Not Achieved |

* EG08 - Optimization of internal business process functionality

|  |  |  |
| --- | --- | --- |
| **Metric** | **Importance** | **Rating** |
| Satisfaction levels of customers with service delivery capabilities | 8 | Largely Achieved |
| Satisfaction levels of suppliers with supply chain capabilities | 8 | Largely Achieved |
| Satisfaction levels of board and executive management with business process capabilities | 4 | Partially Achieved |

* EG08 - Optimization of internal business process functionality

|  |  |  |
| --- | --- | --- |
| **Metric** | **Importance** | **Rating** |
| Percent of business transformation programs with regular reported status updates | 7 | Largely Achieved |
| Percent of business transformation programs stopped | 5 | Partially Achieved |
| Number of programs on time and within budget | 4 | Partially Achieved |
| Percent of stakeholders satisfied with program delivery | 3 | Partially Achieved |

1. **Alignment goal compliance (75%)**
   1. This governance objective supports the achievement of a set of primary alignment goals and metrics:

* AG01 - I&T compliance and support for business compliance with external laws and regulations

|  |  |  |
| --- | --- | --- |
| **Metric** | **Importance** | **Rating** |
| Number of IT-related noncompliance issues reported to the board, or causing public comment or embarrassment | 8 | Largely Achieved |
| Number of noncompliance issues relating to contractual agreements with IT service providers | 8 | Largely Achieved |
| Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss | 6 | Largely Achieved |

* AG03 - Realized benefits from I&T-enabled investments and services portfolio

|  |  |  |
| --- | --- | --- |
| **Metric** | **Importance** | **Rating** |
| Percent of I&T-enabled investments for which claimed benefits in the business case are met or exceeded | 10 | Fully Achieved |
| Percent of I&T services for which expected benefits (as stated in service level agreements) are realized | 6 | Largely Achieved |

1. **Process compliance (57%)**

Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.

* 1. EDM01.01 - Evaluate the governance system

Continually identify and engage with the enterprise’s stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T

|  |  |  |  |
| --- | --- | --- | --- |
| **Maturity Level** | **Activity** | **Importance** | **Rating** |
| 2 | Determine the implications of the overall enterprise control environment with regard to I&T. | 5 | Partially Achieved |
| 3 | Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprises direction, goals and objectives. | 5 | Partially Achieved |
| 2 | Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design | 4 | Partially Achieved |

Related Guidance compliance (Standards, Frameworks, Compliance Requirements)

|  |  |  |  |
| --- | --- | --- | --- |
| **Related Guidance** | **Detailed Reference** | **Importance** | **Rating** |
| National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018 | 3.1 Preparation (Tasks 2, 3, 4, 5) | 8 | Largely Achieved |
| ITIL V3, 2011 | Service Strategy, 2.3 Governance and management systems | 4 | Partially Achieved |

3.2 EDM01.02 - Direct the governance system.

Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making

|  |  |  |  |
| --- | --- | --- | --- |
| **Maturity Level** | **Activity** | **Importance** | **Rating** |
| 2 | Determine the implications of the overall enterprise control environment with regard to I&T. | 5 | Partially Achieved |
| 3 | Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprises direction, goals and objectives. | 5 | Partially Achieved |
| 2 | Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design | 4 | Partially Achieved |

Related Guidance compliance (Standards, Frameworks, Compliance Requirements)

|  |  |  |  |
| --- | --- | --- | --- |
| **Related Guidance** | **Detailed Reference** | **Importance** | **Rating** |
| National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018 | 3.1 Preparation (Tasks 2, 3, 4, 5) | 8 | Largely Achieved |
| ITIL V3, 2011 | Service Strategy, 2.3 Governance and management systems | 4 | Partially Achieved |

3.3 EDM01.03 - Monitor the governance system.

Monitor the effectiveness and performance of the enterprise’s governance of I&T. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of I&T to enable value creation.

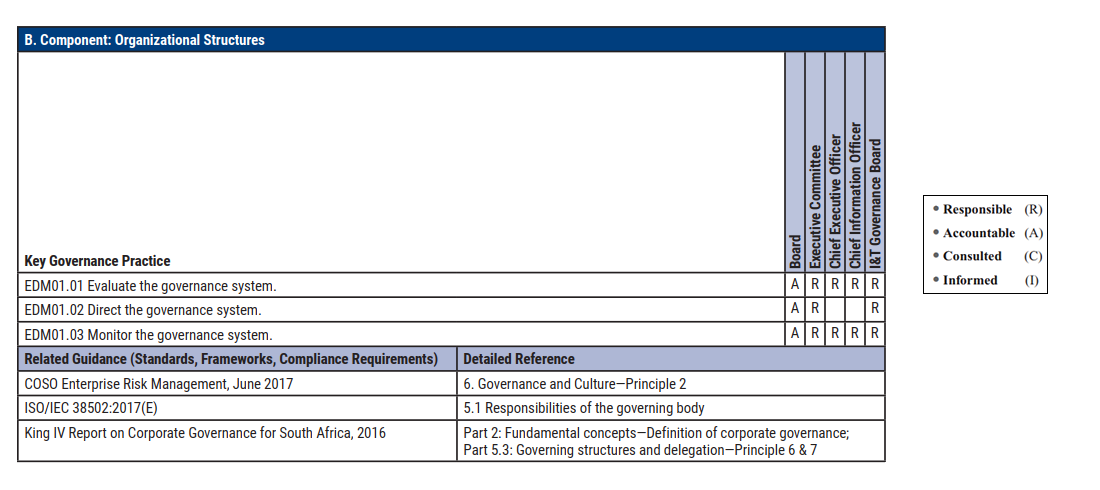
|  |  |  |  |
| --- | --- | --- | --- |
| **Maturity Level** | **Activity** | **Importance** | **Rating** |
| 2 | Determine the implications of the overall enterprise control environment with regard to I&T. | 5 | Partially Achieved |
| 3 | Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprises direction, goals and objectives. | 5 | Partially Achieved |
| 2 | Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design | 4 | Partially Achieved |

Related Guidance compliance (Standards, Frameworks, Compliance Requirements)

|  |  |  |  |
| --- | --- | --- | --- |
| **Related Guidance** | **Detailed Reference** | **Importance** | **Rating** |
| National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018 | 3.1 Preparation (Tasks 2, 3, 4, 5) | 8 | Largely Achieved |
| ITIL V3, 2011 | Service Strategy, 2.3 Governance and management systems | 4 | Partially Achieved |

1. **Organisational structure compliance (67%)**

Organizational structures are the key decision-making entities in an enterprise



|  |  |  |  |
| --- | --- | --- | --- |
| **Sub-Component** | **Regarding the Organisational Structures above. For each management practice, look at the roles and responsibilities diagram according to your organisational context, and select a level of importance/relevance:** | **Importance** | **Rating** |
| EDM01.03 | Roles, responsibilities and authorities are defined, assigned and accepted by appropriate Business Management, IT Management and the Board. | 9 | Fully Achieved |
| EDM01.02 | Roles, responsibilities and authorities are defined, assigned and accepted by appropriate Business Management, IT Management and the Board. | 4 | Partially Achieved |
| EDM01.01 | Roles, responsibilities and authorities are defined, assigned and accepted by appropriate Business Management, IT Management and the Board. | 3 | Partially Achieved |

1. **Information Flow compliance (69%)**

Information is pervasive throughout any organization and includes all information produced and used by the enterprise. COBIT focuses on information required for the effective functioning of the governance system of the enterprise.

5.1 EDM01.01 - Evaluate the governance system.

|  |  |  |  |
| --- | --- | --- | --- |
| **EDM01.01 received the following inputs from upstream processes** | | | |
| **Description** | **From** | **Importance** | **Rating** |
| Constitution/bylaws/ statutes of organization Governance/decision- making model Laws/regulations Business environment trends | Outside COBIT | 6 | Largely Achieved |
| Communications of changed compliance requirements | MEA03.02 | 3 | Partially Achieved |

|  |  |  |  |
| --- | --- | --- | --- |
| **EDM01.01 generated the following outputs, and outputs were forwarded to all relevant down-stream processes.** | | | |
| **Description** | **To** | **Importance** | **Rating** |
| Authority levels | All EDM; APO01.05 | 9 | Fully Achieved |
| Enterprise governance guiding principles | All EDM; APO01.01; APO01.03 APO01.04 | 5 | Partially Achieved |
| Decision-making model | All EDM; APO01.01; APO01.04 | 4 | Partially Achieved |

5.2 EDM01.02 - Direct the governance system

|  |  |  |  |
| --- | --- | --- | --- |
| **EDM01.02 received the following inputs from upstream processes** | | | |
| **Description** | **From** | **Importance** | **Rating** |
| Constitution/bylaws/ statutes of organization Governance/decision- making model Laws/regulations Business environment trends | Outside COBIT | 6 | Largely Achieved |
| Communications of changed compliance requirements | MEA03.02 | 3 | Partially Achieved |

|  |  |  |  |
| --- | --- | --- | --- |
| **EDM01.02 generated the following outputs, and outputs were forwarded to all relevant down-stream processes.** | | | |
| **Description** | **To** | **Importance** | **Rating** |
| Authority levels | All EDM; APO01.05 | 9 | Fully Achieved |
| Enterprise governance guiding principles | All EDM; APO01.01; APO01.03 APO01.04 | 5 | Partially Achieved |
| Decision-making model | All EDM; APO01.01; APO01.04 | 4 | Partially Achieved |

5.3 EDM01.03 - Monitor the governance system.

|  |  |  |  |
| --- | --- | --- | --- |
| **EDM01.03 received the following inputs from upstream processes** | | | |
| **Description** | **From** | **Importance** | **Rating** |
| Constitution/bylaws/ statutes of organization Governance/decision- making model Laws/regulations Business environment trends | Outside COBIT | 6 | Largely Achieved |
| Communications of changed compliance requirements | MEA03.02 | 3 | Partially Achieved |

|  |  |  |  |
| --- | --- | --- | --- |
| **EDM01.03 generated the following outputs, and outputs were forwarded to all relevant down-stream processes.** | | | |
| **Description** | **To** | **Importance** | **Rating** |
| Authority levels | All EDM; APO01.05 | 9 | Fully Achieved |
| Enterprise governance guiding principles | All EDM; APO01.01; APO01.03 APO01.04 | 5 | Partially Achieved |
| Decision-making model | All EDM; APO01.01; APO01.04 | 4 | Partially Achieved |

1. **People, skills and competency compliance (68%)**

People, skills and competencies are required for good decisions, execution of corrective action and successful completion of all activities.

|  |  |  |  |
| --- | --- | --- | --- |
| **Skills** | **Related Guidance (Standards, frameworks, Compliance Requirements)** | **Importance** | **Rating** |
| IS governance | e-Competence Framework (e-CF)A common European Framework for ICT Professionals in all industry sectorsPart 1: Framework, 2016 | 6 | Largely Achieved |
| IT governance | Skills Framework for the Information Age V6, 2015 | 6 | Largely Achieved |

1. **Principles, policies and framework compliance (68%)**

Principles, policies and frameworks translate desired behavior into practical guidance for day-to-day management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Relevant policy** | **Policy Description** | **Related Reference** | **Importance** | **Rating** |
| Delegation of authority policy | Specifies the authority that the board strictly retains for itself. Enumerates general principles of delegation of authority and schedule of delegation (including clear boundaries). Defines organizational structures to which the board delegates authority. | (1) 5.2 Principle 1: Responsibility; (2) 5.3 Delegation; (3) Part 5.3: Governing structures and delegation Principle8 and 10 | 6 | Largely Achieved |
| Governance policy | Provides guiding principles of governance (e.g., I&T governance is critical to enterprise success; I&T and the business align strategically; business requirements and benefits determine priorities; enforcement must be equitable, timely and consistent; industry best practices, frameworks and standards must be assessed and implemented as appropriate). Includes governance imperatives, such as building trust and partnerships, to be successful. Emphasizes that I&T governance reflects a process of continual improvement and must be tailored, maintained and updated to ensure relevance. | 3.14 Planning (PL-1) | 6 | Largely Achieved |

1. **Culture, ethics and behavior compliance (68%)**

Culture, ethics and behavior of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Culture Element** | **Detailed & Related Reference** | **Importance** | **Rating** |
| Identify and communicate the decision-making culture, organizational ethics and individual behaviors that embody enterprise values. Demonstrate ethical leadership and set the tone at the top. | (1) 3.14 Planning (PL-4); (2) 4.1 Principles; (3) Part 5.1: Leadership, ethics and corporate citizenship - Principle 2 | 7 | Largely Achieved |

1. **Services, infrastructure, and applications compliance (56%)**

Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with the governance system for I&T processing

|  |  |  |
| --- | --- | --- |
| **Description** | **Importance** | **Rating** |
| Equivalent frameworks and standards | 8 | Largely Achieved |
| COBIT and related products/tools | 4 | Partially Achieved |