| EmployeeNo: | CMA0213 | CMA | | Performance Year: | 2020/2021 |
|---|---|---|---|---|---|
| Employee Name: | DOUGLAS NGERE | P.o Box: 74800 -00100 Nairobi | | Print Date: | 13-April-2023 |
| Directorate: | Directorate of Technology,Research&Knowledge Mgt | Telephone: +254722 207767 | | | |
| Departmennt: | Information Communication Technology(ICT) | Email: corporate@cma.or.ke | | | |

## Look Forward Report

| Major Requirement | Department Object | Expected Results | Weighted Percentage | Approval Status |
|---|---|---|---|---|
| **Work Plan Objective** | | | | |
| Management and maintenance offi Backups and replication offi the mission critical systems and the Disaster Recovery process | To support Business Continuity process through a robust Disaster Recovery Plan (DRP) | (i) Successfiul backups ffior critical systems and data | 7.50 | Approved |
| | | (ii) Successfiul restores ffior lost infformation or data | | |
| | | (iii) Successfiul ffaiover and ffiallback offi critical systems | | |
| | | (iv) Healthy state offi systems and infformation at the Disaster Recovery site | | |
| Management offi Security offi the ICT inffrastructure | To secure ICT systems, Applications and Data | (i) Authentication and authorization offi valid users in accessing ICT resources | 7.50 | Approved |
| | | (ii) Secure browsing environment | | |
| | | (iii) Secure remote VPN access to system resources | | |
| | | (iv) Restriction offi malware, virus and spyware content | | |
| | | (v) Reduced cybersecurity threats | | |
| | | (vi) Awareness offi the cybersecurity threats by Staffi | | |
| Management offi the Internet, Network, Server, Email and Active Directory Inffrastructure | To guarantee availability offi a reliable ICT inffrastructure | (i) Availability offi centralized authentication and authorization when accessing domain resources | 7.50 | Approved |
| | | (ii) Availability offi the Network inffrastructure ffior availability offi resources | | |
| | | (iii) Availability offi the server inffrastructure ffior availability offi resources | | |
| | | (iv) Availability offi the Messaging (Email) Inffrastructure | | |
| | | (v) Availability offi the telephony inffrastructure | | |
| | | (vi) Availability offi the Internet resource, point-to-point links and site-to-site VPNs | | |
| Updating the Perfformance Management and ICT Risks on PPRMIS | To operate a controlled ICT environment through appropriate Policies and Governance | (i) Aligned and updated workplan based on progress made | 7.50 | Approved |
| | | (ii) Updated ICT enterprise risks with requisite treatment actions | | |
| | | (ii) Discovery offi opportunities and new risks as a result offi the risk management process | | |
| **Business Capability** | | | | |
| Effiective Communication | To secure ICT systems, Applications and Data | Reduced cybersecurity threat opportunities | 10.00 | Approved |
| Innovation and Continuous Improvement | To secure ICT systems, Applications and Data | Enhanced cybersecurity through added layer offi authentication | 10.00 | Approved |
| **Technical Capability** | | | | |
| STG 2 - Risk Management | To operate a controlled ICT environment through appropriate Policies and Governance | Coherent and effective management and implementation offi risk management methods | 6.00 | Approved |
| TEC 1 – Technology Management | To increase automation levels offi internal processes through inffrastructure, systems and applications configures | Ability to expertly install, configure and administer the network and server systems ffior improved perffiormance and security, availability and dependability. | 8.00 | Approved |
| TEC 3 – Technological Strategy | To operate a controlled ICT environment through appropriate Policies and Governance | Delivery offi a cost effective, efficient and sustainable ffiramework to be adopted by the market players and enhance the Authority's market surveillance role | 6.00 | Approved |
| **SpecialObjective** | | | | |
| Development offi a Cybersecurity Framework | To secure ICT systems, Applications and Data | (i) Structured governance and management offi cybersecurity threats | 6.00 | Approved |
| | | (ii) Enhanced ICT security posture | | |
| | | (iii) Improved detection and mitigation offi cyber threats | | |
| Management offi the new Internet Services upon renewal offi contracts | To guarantee availability offi a reliable ICT inffrastructure | (i) Availability offi internet, point-to-point links and DR collocation services affiter November 30th 2020 | 6.00 | Approved |
| Migration offi the DR equipment ffirom the primary site to the DR site | To support Business Continuity process through a robust Disaster Recovery Plan (DRP) | (i) Backup and replication offi the critical systems offisite | 6.00 | Approved |
| | | (ii) Ability to access ICT resources ffirom a remote location | | |
| Participate in the Business Continuity Plan implementation | To support Business Continuity process through a robust Disaster Recovery Plan (DRP) | (i) Structured management and response offi disasters that may disrupt business | 6.00 | Approved |
| | | (ii) Preparedness in handling disasters that may disrupt operations | | |

1

| Major Requirement | Department Object | Expected Results | Weighted Percentage | Approval Status |
|---|---|---|---|---|
| Upgrade the Active Directory Domain Services | To increase automation levels offi internal processes through inffirastructure)system and application upgrades | (i) Enhanced security offi the Active Directory Inffirastructure | 6.00 | Approved |
| | | (ii) Removal offi obsolete windows operating environment | | |
| | | (iiI) Improved ffieatures ffior authorization and accounting | | |
| **Individual Development Plan** | | | | |
| Management offi the Huawei Storage systems | I am responsible ffior the server and storage inffirastructure. The newly acquired inffrastructure supports the entire critical ICT resources. | Frodial Learning | 0.30 | Approved |

**Employee:**            DOUGLAS NGERE

**Employee Signature:**

**SupervisorName:**

**Supervisor Signature**