



Consolidated Performance Risk Management Report

[For October - December (Quarter 2),2019-2020]

-
DCS

Background

The main objective of the established Enterprise Risk Management (ERM) framework is to ensure alignment of strategy, processes, people, technology and funds in order to identify, evaluate and manage opportunities, uncertainties and threats in a structured and disciplined manner and geared towards achieving strategic objectives.

As part of the reporting requirements contained in the Risk Management Policy and Procedures, Management is mandated to report on a periodic basis to the Board on the extent of implementation of risk management strategies. This report presents progress made in the implementation of risk mitigation strategies established under the Enterprise Risk Management Framework that was adopted by the Board in August 2017. Presented below is the risk assessment and ranking methodology adopted;

Risk Impact Rating And Score

Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
An event that, if it occurs would have no effect on the achievement of the targets set	An event that, if it occurs, will cause small cost (and/or schedule) increases that, in most cases, can be absorbed by the activity, project or department	An event that, if it occurred, would cause moderate cost and schedule increases, but important requirements would still be met	An event that, if it occurred, would cause major cost and schedule increases. Secondary requirements may not be achieved	The regulatory or statutory standing of the Authority is brought into serious question or the project is terminated

Opportunity Impact Rating And Score

Insignificant 1	Minor 2	Moderate 3	Major 4	Transformational 5
An opportunity that if it materializes would have no noticeable effect on the achievement of the targets set.	An opportunity that if it materializes would yield a small cost and/or schedule saving to an activity, project or department	An opportunity that if it materializes would yield a moderate cost and/or schedule savings and would enhance the achievement of important requirements	An opportunity that if it materializes would yield a major cost and/or schedule savings and would greatly enhance the achievement of important and secondary requirements	An opportunity that if it materializes would greatly transform the strategic impact of the Authority and the continued realization of its strategic mandate.

Risk/ Opportunity Likelihood Rating and Score

Probability	Description	Risk Score	Opportunity Score	Consideration
Almost Certain	90% or greater chance of the event occurring during the life of the objective	5	5	The risk/ opportunity event has occurred during the last 3-6 months or is certain to occur in the next 3-6 months
Highly Likely	65% to 90% chance of the event occurring during the life of the objective	4	4	There is a history of frequent occurrence. The risk/ opportunity event has occurred during the last 6-12 months or may occur in the next 6-12 months
Likely	35% to 65% chance of the event occurring during the life of the objective	3	3	There is a history of casual occurrence. The risk/ opportunity event has occurred during the last 12-36 months or may occur in the next 12-36 months
Unlikely	10% to 35% chance of the event occurring during the life of the objective	2	2	The risk/ opportunity event occurs from time to time. The event has occurred during the last 36-60 months or may occur in the next 36-60 months
Rare	Less than 10% chance of the event occurring during the life of the objective	1	1	The risk/ opportunity event has not occurred in CMA but has occurred in other similar organizations. The risk event may occur beyond the next 60 months

Overall Risk Rating

Impact	Catastrophic 5	5	10	15	20	25
	Major 4	4	8	12	16	20
	Moderate 3	3	6	9	12	15
	Minor 2	2	4	6	8	10
	Insignificant 1	1	2	3	4	5
		Rare 1	Unlikely 2	Likely 3	Highly Likely 4	Almost Certain 5
		Likelihood				

Risk Treatment Decision

Overall Score	Overall Rating	Risk Treatment Decision
20-25	Very High	Extensive management essential
10-16	High	Management effort required
5-9	Medium	Management effort worthwhile
3-4	Low	Risk may be worth accepting while monitoring
1-2	Very Low	Accept

Overall Opportunity Rating

Impact	Transformational 5	5	10	15	20	25
	Major 4	4	8	12	16	20
	Moderate 3	3	6	9	12	15
	Minor 2	2	4	6	8	10
	Insignificant 1	1	2	3	4	5
		Rare 1	Unlikely 2	Likely 3	Highly Likely 4	Almost Certain 5
		Likelihood				

Opportunity Treatment Decision

Overall Score	Overall Rating	Opportunity Treatment Decision
20-25	Very High	Extensive management effort essential to harness opportunity
10-16	High	Management effort required to actualize opportunity
5-9	Medium	Management effort worthwhile to pursue opportunity
3-4	Low	Opportunity worth monitoring
1-2	Very Low	Opportunity worth noting

Cumulative Risks with Cumulative Activities:

N O	Strategic Objective	Cumulative Risk	Cumulative Activity	Expected Cumulative Outcome
1	Ensure optimal institutional efficiency and effectiveness of CMA	KRA and the National Treasury seizing Authority Reserves and placing agency notices on bank accounts. 25	High level engagement with KRA on basis of reservation and commitment of funds held by the Authority, while promptly settling amounts deemed genuinely due against 90% surplus obligation. 93 %	Continued funding of operations and safety of ICF funds.
2	Ensure optimal institutional efficiency and effectiveness of CMA	Non compliance with Procurement, financial and Human Resource laws, policies and procedures, guidelines and circulars 20	Continued sensitisation of staff and enforcement of laid down procedures and reporting requirements. 90 %	Maintain institutional integrity and reputation
3	Leveraging technology to drive efficiency in the capital markets value chain	Obsolescence of server hardware equipment and systems software 20	Upgrades are at different stages of implementation 28 %	Improved infrastructure, capacity, performance and security of Information systems.
4	Ensure optimal institutional efficiency and effectiveness of CMA	Cyber security threats 20	Development and implementation of appropriate Cybersecurity frameworks 38 %	Confidentiality, continued availability and integrity of data and information.
5	Ensure optimal institutional efficiency and effectiveness of CMA	Failure of 3rd party ICT service providers 20	Review and ensure effective back up arrangements are in place and that SLAs with providers carry penalty clauses. 75 %	99.9% Reliability and availability of contracted services.
6	Ensure optimal institutional efficiency and effectiveness of CMA	Reduced capability of the Authority from declining staff engagement and headcount shortage. 20	Deployed teams to address urgent strategic issues and continue to pursue the National Treasury and SCAC for an expedited approval of revised HR instruments. 40 %	Optimal institutional capacity and effectiveness



Cumulative Risks heatmap




Impact	Catastrophic 5				DCS13 DCS17	DCS18
	Major 4					DCS14 DCS15 DCS16
	Moderate 3					
	Minor 2					
	Insignificant 1					
		Rare 1	Unlikely 2	Likely 3	Highly Likely 4	Almost Certain 5
		Likelihood				

No	Cumulative Risk	Score	Ref No
1	KRA and the National Treasury seizing Authority Reserves and placing agency notices on bank accounts.	25	DCS18
2	Non compliance with Procurement, financial and Human Resource laws, policies and procedures, guidelines and circulars	20	DCS13
3	Obsolescence of server hardware equipment and systems software	20	DCS14
4	Cyber security threats	20	DCS15
5	Failure of 3rd party ICT service providers	20	DCS16
6	Reduced capability of the Authority from declining staff engagement and headcount shortage.	20	DCS17

Detailed Status of Risks

#	Description	Current Rating	Prior Rating	Risk Drivers	Risk Management Strategy Undertaken	Effect of Risk to Authority	Action to be Undertaken	Person Responsible
1	Obsolescence of server hardware equipment and systems software at the Authority	25 (5*5) ← ● →	25 (5*5)	<ul style="list-style-type: none"> - Continuous release of new hardware infrastructure, Operating system, Application and/or Database software by system owners/vendors - Continuous use of old server and storage hardware equipment 	<ul style="list-style-type: none"> - 1. Effective patching of all the operating systems, application and database management system software nearing end-of-life 2. Project initiation between CMA and Attain on the upgrade of Enterprise systems, applications and operating system software 3. Received the licenses for the respective operating system software and enterprise applications from the vendor Attain 4. Developed a low-level design document that will be used in the software upgrades - 1. Timely replacement of failed hardware infrastructure peripherals such as hard disks and power supply units 2. Project initiation between CMA and Computech on the server hardware upgrade 3. Conducted current server 	<ul style="list-style-type: none"> - 1.Exposing the ICT resources to zero day attacks 2. Running application or server platforms not support by vendor security/critical updates 	<ul style="list-style-type: none"> - 1. Continuous patching of current operating systems, application or database software using the Windows Server Update Services (WSUS) 2. Upgrade of the operating system software, Database management systems, email infrastructure and enterprise applications to the most current versions available - 1. Maintenance and management of the right operating environment in terms redundant power supply and adequate cooling at the server room 2. Timely repair of failed or faulty peripherals in the current server hardware 3. Installation, setup and configuration of a new storage and server hardware 	

					infrastructure review and developed a low level design document that will guide the hardware upgrade 4. Procured 6 additional blade servers for use in the expected storage infrastructure		at the Primary data center and DR sites respectively 4. Migration of the enterprise applications and systems from the current obsolete hardware to the new hardware infrastructure	
2	Delayed approval of Human Resource Instruments	25 (5*5) 	20 (5*4)	- Lengthy process of approving the Human Resource Instruments by the National Treasury	- The Authority engaged with SCAC to review CMA HR Instruments in a retreat held in Naivasha for one week. Approval of the instruments by The National Treasury is awaited.	- Low staff morale. Failure to achieve key targets.	- Continuous Board engagement with relevant authorities for approval.	
3	Ineffective succession planning	20 (4*5) 	20 (4*5)	- Failure to afford the right talent	- Board engagement with the National Treasury	- Business continuity may be hampered Low staff morale when they act in higher roles for long duration	- Review of succession planning matrix across the organization	

4	Failure of 3rd party ICT service providers	20 (4*5) 	20 (4*5)	- 1. Fiber cuts 2. Domain Naming Service (DNS) failure on the provider's servers which hosts our domain (cma.or.ke) 3. Configuration changes from the service providers end	- 1. Maintenance of two separate independent internet links	- 1. Inability to send or receive external emails 2. Unavailability of the CMA website	- 1. Continue to maintain and manage the two independent internet links for redundancy 2. Manage and maintain valid contracts for the provision of Internet, Domain and web hosting services 3. Require KenyaWeb to implement redundancy on their DNS servers	
5	Non compliance with the Procurement Plan requirements and procurement procedures	20 (4*5) 	12 (4*3)	- 1. Departmental plans not drawn from the budget 2. Users circumventing the procurement process 3. User specifications not clear/well drawn 4. Short time frames provided by users to deliver services/goods	- The user departments have already been engaged to ensure submission of the departmental procurement plans	- Delayed delivery of goods and services, Warnings and/or sanctions from PPRA Loss of funds	- Sensitization and Monitoring	
6	Inadequate Financial Resources.	20 (4*5) 	20 (4*5)	- Low Market Turnover. -	- Spending within revenue collected revenue Prioritizing strategic plan activities	- Lack of delivery of mandate	- Facilitate Market deepening - Facilitate uptake of existing products through market deepening	
							- 1. Maintain a robust email spam filtering solution 2. Maintain an updated and licensed enterprise anti-virus 3. Send out monthly ICT security tips to staff 4.	

7	Cyber security threats	20 (5*4) ← ● →	20 (5*4)	<ul style="list-style-type: none"> - 1. Ransomware such as Wannacry, Locky etc 2. Viruses, spyware, spam and other forms of malware 3. Phishing and pharming - Unpatched client and server operating systems - Social engineering through malicious email - Unauthorized access to critical systems or data 	<ul style="list-style-type: none"> - 1. Maintained an effective web filtering solution 2. Maintained a robust email spam filtering solution 3. Maintained an effective end-point security solution 4. Maintained an effective backup process for critical data - Maintained an effective patch management program for client and server systems - Conducted user awareness on current threats - Managed and maintained the principle of least privilege in granting access to ICT resources Monitored the respective critical aspects of the ICT infrastructure 	<ul style="list-style-type: none"> - 1. Data corruption and/or loss 2. Data theft 3. Breach of employee privacy 4. Reputation damage as a result of succesful data breaches - Data loss and/or data corruption through zero-day attacks - Users clicking on malicious links or attachments sent on email or other mediums to enable a successful attack - 1. Privilege escalation 2. Data loss 3. Unauthorized access to confidential information 	<ul style="list-style-type: none"> Maintain a successful backup solution and process 5. Maintain an effective web filtering solution 6. Maintain and manage an effective perimeter firewall with relevant patches 7. Acquire a Security Incident and Event Management systems (SIEM) and Network Access Control for indedpth network and systems monitoring for the detection and prevention of vulnerabilities and threats - Maintain an effective patch management program for client and server systems - Continue to sensitize staff on the evolving cyber security threat landscape - 1. Review of user profiles assigned to staff on the enterprise systems 2. Review of the Domain Admins membership 3. Review of staff access to the file server systems
---	------------------------	----------------------	-------------	---	---	---	---

