Office of Inspector General
for the Millennium Challenge Corporation

June 1, 2011

Mr. Daniel W. Yohannes
Chief Executive Officer
Millennium Challenge Corporation
875 Fifteenth Street, N.W.
Washington, DC 20005

Dear Mr. Yohannes:

Enclosed is the final report on the *Risk Assessment of the Millennium Challenge Corporation's Information Technology Governance Over Its Information Technology Investments* (Report No. M-000-11-001-O). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of Clifton Gunderson LLP (Clifton Gunderson) to conduct the risk assessment. Clifton Gunderson conducted their risk assessment in accordance with United States Generally Accepted Government Auditing Standards, as amended.

Clifton Gunderson determined that MCC's information technology (IT) governance processes for the selected IT governance areas ranged from maturity level ratings of *Initial/Ad hoc* through *Managed and Measurable*. Weaknesses in MCC's IT governance processes may increase IT project costs, lengthen deployment, and deliver solutions that do not satisfy business needs.

As MCC continues to select and manage its information technology investments, it is important to correct weakness and to have formal IT governance. This will assist in ensuring IT objectives are correlated with business objectives and IT investments are prioritized and managed to effectively support Agency initiatives. Therefore, Clifton Gunderson's report makes 23 recommendations to help MCC achieve an appropriate level of information technology governance and control. In addition, Clifton Gunderson's report makes 17 suggestions to help MCC implement best practices which are of lesser priority. Although OIG will not formally track the suggestions, MCC should consider prioritizing and implementing them, as appropriate.

In carrying out its oversight responsibilities, the OIG reviewed Clifton Gunderson's report and related risk assessment documentation. The OIG's review, as differentiated from an

audit in accordance with U.S. Generally Accepted Government Auditing Standards, was not intended to enable the OIG to express, and we do not express an opinion on MCC's IT governance over its IT investments. Clifton Gunderson is responsible for the enclosed risk assessment report and the conclusions expressed therein. However, our review disclosed no instances that Clifton Gunderson did not comply, in all material respects, with applicable standards.

To address the weaknesses reported by Clifton Gunderson, OIG is making the following recommendations to MCC's management:

Recommendation 1: *We recommend that the Millennium Challenge Corporation Chief Information Officer update the information technology strategic plan to reflect current enterprise strategic goals.*

Recommendation 2: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a formal process for managing risk and updating the information technology strategic plan accordingly. Risk management must drive enterprise architecture decisions, providing secure information system environments for critical applications. The plan should be reviewed at a minimum annually and when major events occur that have an impact on strategic goals. When updating the information technology strategic plan the Chief Information Officer should verify compliance with the Office of Management and Budget Circular No. A-130, Management of Federal Information Systems, with regard to the capital planning and investment control process which includes the information resource management strategic plan and the information technology capital plan which is required to be updated twice yearly.*

Recommendation 3: *We recommend that the Millennium Challenge Corporation Chief Information Officer complete the enterprise information architecture planning and implementation project as discussed in the* Executive Level Notional OCIO 2 Year Portfolio *in order to maintain an information architecture that reflects the business requirements.*

Recommendation 4: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a project plan for leveraging data as indicated in the authoritative data source process and methodology in order to provide business users access to detailed information to aid in analysis and decision making.*

Recommendation 5: *We recommend that the Millennium Challenge Corporation Chief of Staff develop and implement a formal process that must be consistently ap*plied *for the Enterprise Architecture Steering Committee to prioritize information technology-enabled investment programs.*

Recommendation 6: *We recommend that the Millennium Challenge Corporation Chief of Staff formally document and implement a process requiring the Enterprise Architecture Steering Committee to consider risk management when discussing strategic direction and approval of information technology investments.*

***Recommendation 7**: We recommend that Millennium Challenge Corporation Chief Information Officer (1) conduct an analysis to determine whether the information technology function has sufficient resources to adequately support the business goals and objectives of the organization and (2) through the organization's budgeting process, submit a written request for additional resources to address any shortfalls identified in the analysis.*

***Recommendation 8:** We recommend that the Millennium Challenge Corporation Deputy Chief Financial Officer revise the budget policy and procedures to account for the change from line item budgeting to project budgeting.*

***Recommendation 9:** We recommend that the Millennium Challenge Corporation Chief Information Officer develop a process and implement a tool for monitoring project plans and work completed to determine earned value, providing an early warning of performance issues impacting project budgets.*

***Recommendation 10:** We recommend that the Millennium Challenge Corporation Chief Information Officer define quality requirements, criteria, and key performance indicators for evaluation of quality management for key information technology processes.*

***Recommendation 11:** We recommend that the Millennium Challenge Corporation Chief Information Officer identify and document standards, procedures, and practices for key information technology processes to guide the Agency in defining and evaluating criteria for quality management.*

***Recommendation 12:** We recommend that the Millennium Challenge Corporation Chief Information Officer implement a process to incorporate the following components into its projects:*

- *A project governance structure that includes the roles, responsibilities, and accountabilities of various key players in project management.*
- *Project sponsors assigned for the execution of each project.*
- *Project office and project manager.*
- *Elements such as approving the initiation of phases, communicating to all stakeholders the status of projects, establishing an integrated project plan, project quality plan, and defining the responsibilities of project team members.*
- *Project risk management through the process of planning, identifying, analyzing, responding to, monitoring and controlling risk.*
- *Project change control.*
- *Lessons learned.*

Recommendation 13: *We recommend that the Millennium Challenge Corporation Chief Information Officer implement a process to verify that risk management plans and Exhibit 300 business cases are consistently used, monitored and updated annually for all information technology projects as required.*

Recommendation 14: *We recommend that the Millennium Challenge Corporation Chief Information Officer finalize and implement the system development life cycle.*

Recommendation 15: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a policy to fully address the maintenance of software applications.*

Recommendation 16: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process for ensuring the integration of software into the current infrastructure is properly planned and executed.*

Recommendation 17: *We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement information technology acquisition instructions that provide a methodology to evaluate the components of information technology acquisition contracts.*

Recommendation 18: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process to ensure end user testing and evaluation of developed applications.*

Recommendation 19: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process to ensure personnel are trained in the use of developed applications.*

Recommendation 20: *We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement policies and procedures for data conversion, testing of applications and infrastructure migration.*

Recommendation 21: *We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement a process to enforce the creation of service level agreements for all endeavors requiring contract support.*

Recommendation 22: *We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement a process for periodic review and feedback of performance for all contractors to improve service delivery and support early detection of potential problems.*

Recommendation 23: *We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a monitoring process to ensure that all information technology projects are provided a priority level commensurate with the direction and goals of the Agency as a whole, not with the goals of individual leaders within the Agency.*

Based on Clifton Gunderson's evaluation of MCC's comments, OIG agrees with the management decisions reached on Recommendations 17, 21, and 22. However, MCC could not reach management decisions for the remaining 20 recommendations because MCC has not determined target dates for completing the planned actions. Please provide target dates to address the remaining 20 recommendations within 6 months of the date of this report.

The OIG appreciates the cooperation and courtesies extended to our staff and to the staff of Clifton Gunderson.

Sincerely,

/s/

Alvin A. Brown
Assistant Inspector General
Millennium Challenge Corporation

cc:
Steven M. Kaufmann, Chief of Staff
Victoria B. Wassmer, Vice President, Department of Administration and Finance
Dennis Lauer, Chief Information Officer
Dennis E. Nolan, Deputy Chief Financial Officer
Jim R. Blades, Director of Contracting
Arlene McDonald, Compliance Officer

A1

RISK ASSESSMENT OF THE MILLENNIUM CHALLENGE CORPORATION'S INFORMATION TECHNOLOGY GOVERNANCE OVER ITS INFORMATION TECHNOLOGY INVESTMENTS

May 13, 2011

4250 N. Fairfax Drive
Suite 1020
Arlington, Virginia 22203
tel: 571-227-9500
fax: 571-227-9552

www.cliftoncpa.com

CONTENTS

SUMMARY OF RESULTS

The Millennium Challenge Corporation (MCC) was created by the U.S. Congress in January 2004. MCC is an independent U.S. foreign aid agency that is helping lead the fight against global poverty. A relatively small organization, MCC currently employs approximately 300 personnel, including 7 IT personnel plus contractor support.

Clifton Gunderson (CG) LLP was engaged by the Assistant Inspector General (AIG) for the Millennium Challenge Corporation (MCC) to conduct a risk assessment of MCC's information technology (IT) governance over its IT investments. IT governance provides the structure that links IT processes, resources and information to enterprise strategies and objectives. The objectives are to (1) align IT with the business, enable the business, and maximize resources; (2) use IT resources responsibly; and (3) appropriately manage IT risks.

Our risk assessment focused on MCC's governance process related to selecting, managing and controlling its IT investments. The outcome of our assessment was to identify weaknesses in controls that could impact MCC's ability to align IT risk with the enterprise risk management framework, correlate IT objectives with business objectives, set the tone from the top, make risk based business decisions, and manage IT investments in a manner that is perceived as a value in supporting business initiatives. The objective of the assessment was to answer the following question:

> *What are MCC's risks for selecting, managing and controlling its information technology investments?*

Our assessment resulted in a scorecard for capturing measurements and provides a view of areas where risks may arise in achieving organizational goals and identifying areas for improvement. We determined that MCC's IT governance processes for the selected IT governance areas ranged from maturity level ratings of Initial/Ad hoc through Managed and Measurable. Weaknesses in MCC's IT governance processes may increase IT project costs, lengthen deployment, and deliver solutions that do not satisfy business needs. Closing these control gaps will help ensure MCC achieves maximum benefit from developing an appropriate level of IT governance and control.

The scorecard below summarizes the results of the review:

Millennium Challenge Corporation IT Governance Over its IT Investments							
SCORECARD							
Control Objectives for Information and related Technology (COBIT) Maturity Model							
Maturity Level		**0 - Non-existent**	**1 - Initial/Ad-Hoc**	**2 - Repeatable but Intuitive**	**3 - Defined Process**	**4 - Managed and Measurable**	**5 - Optimized**
Planning and Organization							
PO1	Define a Strategic Plan				X		
PO2	Define the Information Architecture			X			
PO4	Define the IT Processes, Organization and Relationships			X			
PO5	Manage the IT Investment				X		
PO8	Manage Quality		X				
PO10	Manage Projects			X			
Acquire and Implement							
AI2	Acquire and Maintain Application Software		X				
AI3	Acquire and Maintain Technology Infrastructure			X			
AI5	Procure IT Resources				X		
AI7	Install and Accredit Solutions and Changes			X			
Deliver and Support							
DS1	Define and Manage Service Levels				X		
DS2	Manage Third Party Services					X	
DS10	Manage Problems					X	
Monitor and Evaluate							
ME1	Monitor and Evaluate IT Performance				X		
ME3	Ensure Compliance with External Requirements					X	
ME4	Provide IT Governance			X			

In addition to identifying the levels of maturity for several areas, we also identified key risk areas, including:

- MCC has not developed and implemented a process for updating its IT Strategic Plan to reflect current enterprise strategic goals;
- MCC has not developed and implemented a process for ensuring risk assessments are performed for all IT projects or continuous monitoring of project risk is occurring;
- MCC has not completed the enterprise architecture planning and implementation project in order to reflect current business requirements;
- MCC has not consistently prioritized IT-enabled investment programs to ensure all IT projects are provided a priority level commensurate with the direction and goals of the Agency as a whole; and
- MCC has not consistently implemented a project governance structure containing the necessary elements to ensure a disciplined project management process.

To address the issues noted above, the report documents both recommendations and suggestions. The recommendations are in support of opportunities for improvement deemed to be of highest priority to close control gaps. The suggestions are deemed to be of lesser priority for ensuring best practices are achieved. The twenty-three recommendations and seventeen suggestions are documented within the discussion regarding each COBIT control area assessed.

In finalizing the report, we received and considered MCC's response to the draft risk assessment report and the recommendations included therein. In its comments, MCC concurred with all of the recommendations, but could not yet provide timelines to address 20 of the 23 recommendations. MCC plans to complete the timelines by July 31, 2011. We agree with MCC's management decisions to address recommendations 17, 21, and 22.

The detailed risk assessment results are discussed in the next section. Appendix I describes the assessment's scope and methodology. Appendix II contains MCC's management comments without attachments.

RISK ASSESSMENT RESULTS

Plan and Organize (PO)

Strategic Planning

The Millennium Challenge Corporation (MCC) maintains an enterprise portfolio of IT-enabled investments in the form of the *Executive Level Notional OCIO Two Year Portfolio*. The portfolio provides a high level view of the milestones, dependencies, decision points and status of each of the IT projects. In addition, an Information Systems Strategic Plan has been developed covering FY08 through FY10 which focuses on realigning performance goals and resources to support a business centric, portfolio management approach. Goals, sub-goals and performance objectives for infrastructure, strategy, systems and capacity are discussed. The Plan outlines the portfolio management process, prioritization of projects, budgeting and the acquisition strategy.

However, the strategic planning process does not include the development of long range plans as the basis for building the IT Strategic Plan. In addition, MCC has not developed and implemented a formal process for managing risk and updating the Strategic Plan accordingly. As a result, the plan has not been maintained and is currently out of date. According to the CIO, the plan is not properly aligned with core business requirements since those requirements have changed over the life of the document. In addition, the plan does not tactically address achievement of the strategic goals. A revised plan is being developed and is scheduled for completion by March of 2011. In addition, MCC is beginning to address risk responsibility at the enterprise level by the newly created position, Senior Investment and Risk Officer under the direction of the Chief Executive Officer (CEO).

IT Processes, Organization and Relationships

MCC has implemented an Enterprise Architecture Steering Committee (EASC) which establishes a process for reciprocal involvement in strategic planning. The EASC aims to align and integrate IT strategies with MCC's business objectives. The EASC charter outlines the three basic tenets of the committee: 1) the EASC should be jointly chaired by a business executive and a technical representative; 2) the EASC is an advisory and implementation body to the Information Management Committee; and 3) direct communication between the EASC team and all levels in the implementation oversight and review process is expected as a means of exchanging information and building trust. The EASC is charged with establishing both project managers and business sponsors of all major Information Technology investments above a $300,000 threshold.

Although the committee provides oversight, a formal process is not in place for the EASC to prioritize IT-enabled investment programs. Initially, little attention was given to the EASC; however, the entrance of the new Chief of Staff has increased its use, effectiveness and frequency of meetings. A Senior Investment and Risk Officer has recently been hired to focus on risks associated with the program functions. While this person is not a member of the EASC, increased focus on risk management by the EASC has begun through the leveraging of the risk methodology and templates established by the Risk Office.

We observed that the reporting line of the CIO does not reflect the importance of IT within the Agency. The CIO has a dotted reporting line to the CEO and a direct line to the CFO. Although the EASC is tasked with providing governance for IT projects and the CIO has begun assigning a project manager to monitor projects, there are situations in which the priorities of the CIO may conflict with the priorities of the CFO. This structure has also led to the IT function lacking resources to adequately support the business goals and objectives. The CIO conducted a benchmarking study this year to determine the appropriate levels of funding within the IT budget, which should assist in the appropriate level of IT staff needed. The benchmarking study indicated that MCC is on the low end of IT spending. Over a three year period, MCC has averaged 10% versus comparable agencies at 11% to 20%. IT resources include both full time equivalent employees and contractors. (We are not making a recommendation to address the position of the Chief Information Officer within the organizational structure. A recommendation was opened from a prior audit[1] and has subsequently been closed by the OIG[2].)

MCC has a process in place to ensure both MCC employees and contract personnel who support the IT function know and comply with MCC's policies for protection of the organization's information assets. In addition, security requirements are outlined in contracts and contract personnel are required to comply with the same personnel security background requirements as MCC employees. However, for the resources available, skill inventories of both IT and business resources are not documented to support staffing for IT projects. Skill inventories would allow project managers to staff projects with the most appropriate subject matter experts throughout the organization. Finally, in addition to the relationship the IT function maintains with the EASC, MCC has developed a communication and liaison structure between the IT function and various other interests outside the IT function, such as the Office of Inspector General (OIG), the Office of Management and Budget (OMB) and the Audit Committee. These relationships help the CIO ensure an understanding and focus on Federal requirements and process improvements.

Defining the Information Architecture

MCC has developed and implemented a data classification scheme, which provides a consistent approach for describing, categorizing and employing MCC data in a standard and consistent manner across the Agency. Core data is used across all of MCC. Common data is used across two working groups or divisions and distinct data is used within one working group or division. In addition, data has been classified according to protection requirements. An enterprise data dictionary or Data Reference Model (DRM) is being completed and is on track for completion by September 2011. This will promote a common understanding of data among IT and business users and allow for the sharing of data elements among applications and systems. The DRM is part of an overall Enterprise Content Management strategy that MCC is in the process of initiating to formalize the organization and storage of data. The approach for the DRM is based on

[1] *Audit of the Millennium Challenge Corporations Implementation of Key Components of a Privacy Program for Its Information Technology Systems* (Report No. M-000-10-003-P, July 10, 2010).

[2] Memorandum from Assistant Inspector General: *Closure of Audit Recommendations 1 and 2 for the Audit of the Millennium Challenge Corporation's Implementation of Key Components of a Privacy Program for Its Information Technology Systems* (Audit Report No. M-000-10-003-P).

the Federal Enterprise Architecture, an initiative of the U.S. Office of Management and Budget that intends to comply with the Clinger-Cohen Act and affords a common methodology for information technology acquisition.

MCC is currently constructing the basic framework of an enterprise architecture lifecycle as documented in the *Executive Level Notional OCIO 2 Year Portfolio*, starting with the Business Reference Model and Data Reference Model. The enterprise information architecture project should assist MCC in further aligning resources to increase business performance and facilitate MCC carrying out its mission. A methodology for leveraging information through data warehouse and data mining technologies has been determined but implementation will not commence until the data dictionary is completed and the ECM project is at a maturity level that would allow for leveraging data.

Managing the IT Investment

MCC has established a detailed manual for IT budget formulation policy and procedures and a budget for IT projects has been established which includes the prioritization of requested activities. A quarterly budget review is performed to refine budgeting requirements based on the status of projects and changing priorities. The decision-making process for prioritizing the allocation of IT resources is based on value and risk as documented in the IT Strategic Plan; however, it is not consistently applied. For example, the highest priority set by IT is the General Support System followed by IT security; however, the process for prioritizing projects established by the business units has not been established. Recently, the budgeting process was modified from line item budgeting to a project based approach. The IT Budget Formulation Policy and Procedure manual has not been updated to reflect this change. Currently there is no clear line of site between budgeting for IT projects and monitoring of project plans in order to determine earned value and provide early warning of performance issues impacting project budgets.

Managing Quality

A Quality Management System (QMS) defines the organizational structure for quality management, covering the roles, tasks and responsibilities. In addition, standards, procedures and practices for key IT processes including development and acquisitions that follow the life cycle of the deliverable should be documented and maintained. The quality of IT services provided at MCC is tracked through an informal quality management process. MCC utilizes quality satisfaction surveying which results in improvement if issues arise. A QMS that identifies quality requirements and criteria, and monitors performance against these requirements and criteria for continuous improvement of IT services is not in place. In addition, MCC has not documented standards, procedures and practices for key IT processes.

Managing Projects

MCC utilizes a portfolio tracker to monitor the status of major IT projects. Individuals responsible for managing IT projects are required to obtain project management certification. However, MCC does not have a project governance structure in place that establishes elements such as a project office, project manager, project sponsors, or steering committee for each project. Additionally, all IT projects do not have the benefit of an assigned sponsor with sufficient authority to own the execution of the project within the overall strategic program. Responsibilities, relationships, authorities, and performance criteria of project team members are not defined and the basis for acquiring

and assigning competent staff members and/or contractors to projects is not specified. Although MCC's contracts include Service Level Agreements (SLAs), its project management approach does not identify key criteria in which project performance of contractors may be measured. The primary stakeholder of projects is usually the business; however, the definition and execution of projects is typically not obtained. The initiation of each major project phase is not approved. In addition, there is no review or acceptance of deliverables of the previous phase nor approval of an updated business case at the next major review of the program. This is the result of lack of consistent project communication with all stakeholders. Although MCC tracks the status of specific milestones on the portfolio tracker, project stakeholders are not required to ascertain whether the project delivered the planned results and benefits. In addition, lessons learned are not documented for use on future projects and programs. The lack of a formal project management structure, including planning, identifying, analyzing, responding to, monitoring and controlling risk, has lead to inconsistent application of management practices for IT projects.

The summary of observations identified in the review as well as the assessed COBIT Maturity Level Ranking and recommendations are provided as follows:

COBIT PO1 - Define a Strategic Plan

Observed Best Practices

1. MCC maintains an enterprise portfolio of IT-enabled investments. The *Executive Level Notional OCIO Two Year Portfolio* provides a high level view of the milestones, dependencies, decision points and status for each of the IT projects.

2. MCC has implemented the Enterprise Architecture Steering Committee (EASC) which establishes a process for reciprocal involvement in strategic planning.

3. An IT Strategic Plan covering FY08 through FY10 was developed which focused on realigning its performance goals and resources to support a business centric, portfolio management approach.

Opportunities for Improvement

1. MCC has not developed and implemented a formal process for managing risk.

2. MCC has not developed and implemented a formal process for updating the IT Strategic Plan to reflect current enterprise strategic goals.

3. The strategic planning process does not include the development of tactical plans to aid in the achievement of the strategic goals or the development of long range plans in order to plan for accomplishing a set of goals over a longer period of time.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 3 – Defined

COBIT Definition - A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach that is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate

planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process, and there are no procedures to examine the process. The overall IT strategy includes a consistent definition of risks that the organization is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly influence the acquisition of new products and technologies. IT strategic planning is discussed at business management meetings.

Recommendations

1. We recommend that the Millennium Challenge Corporation Chief Information Officer update the Information Technology Strategic Plan to reflect current enterprise strategic goals.

2. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a formal process for managing risk and updating the Information Technology Strategic Plan accordingly. Risk management must drive enterprise architecture decisions, providing secure information system environments for critical applications. The plan should be reviewed at a minimum annually and when major events occur that have an impact on strategic goals. When updating the Information Technology Strategic Plan the Chief Information Officer should verify compliance with the Office of Management and Budget Circular No. A-130, *Management of Federal Information Systems,* with regard to the capital planning and investment control process which includes the Information Resource Management Strategic Plan and the Information Technology Capital Plan which is required to be updated twice yearly.

Suggestions

1. We suggest that the Millennium Challenge Corporation Chief Information Officer incorporate tactical planning into the strategic planning process by breaking the strategic plan down into short term actions and plans. A tactical plan contains a list of deliverables, a schedule, resources, a budget and a mapping of how it will be completed.

2. We suggest that the Millennium Challenge Corporation Chief Information Officer develop long range plans as the basis for building the Information Technology Strategic Plan.

COBIT PO2 - Define the Information Architecture

Observed Best Practices

1. MCC has developed and implemented a data classification scheme, which provides a consistent approach for describing, categorizing and employing MCC data in a standard and consistent manner across the Agency.

2. The Enterprise Data Dictionary or Data Reference Model (DRM) is being completed and is on track for completion by spring 2011 which will promote a common understanding of data among IT and business users and allow for the sharing of data

elements among applications and systems. The DRM is part of an overall Enterprise Content Management (ECM) strategy that MCC is in the process of initiating.

Opportunities for Improvement

1. An enterprise information architecture project, as documented in the *Executive Level Notional OCIO 2 Year Portfolio*, is in early stages and needs to be completed in order to further align resources to increase business performance and facilitate MCC carrying out its mission.

2. A methodology for leveraging information (i.e., data warehouse or data mining technologies) has been determined but implementation will not commence until the Enterprise Content Management (ECM) project is at a maturity level to provide business users access to detailed information to aid in analysis and decision making.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 2 – Repeatable but Intuitive

COBIT Definition - An information architecture process emerges and similar, though informal and intuitive, procedures are followed by different individuals within the organization. Staff obtain their skills in building the information architecture through hands-on experience and repeated application of techniques. Tactical requirements drive the development of information architecture components by individual staff members.

Recommendations

3. We recommend that the Millennium Challenge Corporation Chief Information Officer complete the enterprise information architecture planning and implementation project as discussed in the *Executive Level Notional OCIO 2 Year Portfolio* in order to maintain an information architecture that reflects the business requirements.

4. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a project plan for leveraging data as indicated in the authoritative data source process and methodology so as to provide business users access to detailed information to aid in analysis and decision making.

COBIT PO4 - Define the IT Processes, Organizations and Relationships

Observed Best Practices

1. MCC has established an Enterprise Architecture Steering Committee, clearly indicating key positions and roles and responsibilities of the committee.

2. Risk responsibility at the enterprise level is beginning to be addressed by the newly created position, Senior Investment and Risk Officer under the direction of the Chief Executive Officer.

3. MCC has conducted a benchmarking study to determine the appropriate levels of funding within the IT budget, which should ultimately assist in the determination of the appropriate level of IT staff needed.

4. MCC has processes in place for ensuring that consultants and contract personnel who support the IT function know and comply with MCC's policies for the protection of the organization's information assets.

5. MCC has developed a communication and liaison structure between external entities such as the OMB, OIG, External Audit Committee, and private companies.

Opportunities for Improvement

1. A formal process is not in place for the EASC to prioritize IT-enabled investment programs. Additionally, the EASC has not formally implemented a process to focus on risk management considerations.

2. The IT function is not contingent on the importance of IT within the enterprise. Furthermore, the reporting line of the CIO does not reflect the importance of IT. The CIO may have limited power in ensuring IT projects are provided a priority level commensurate with the direction and goals of the Agency as a whole.

3. Skill inventories are not available to support project staffing.

4. The IT function does not have sufficient resources to adequately support the business goals and objectives.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 2 – Repeatable but Intuitive

COBIT Definition - The IT function is organized to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured organization and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organization and vendor relationships.

Recommendations

5. We recommend that the Millennium Challenge Corporation Chief of Staff develop and implement a formal process for the Enterprise Architecture Steering Committee to prioritize Information Technology-enabled investment programs which must be consistently applied.

6. We recommend that the Millennium Challenge Corporation Chief of Staff formally document and implement a process requiring the Enterprise Architecture Steering Committee to consider risk management when discussing strategic direction and approval of information technology investments.

7. We recommend that Millennium Challenge Corporation Chief Information Officer (1) conduct an analysis to determine whether the information technology function has sufficient resources to adequately support the business goals and objectives of the organization and (2) through the organization's budgeting process, submit a written request for additional resources to address any shortfalls identified in the analysis.

Suggestions

3. We suggest that the Millennium Challenge Corporation Chief Information Officer and the MCC Chief Financial Officer develop skill inventories to support staffing for Information Technology projects to include both Information Technology and business resources.

COBIT PO5 - Manage the IT Investment

Observed Best Practices

1. MCC has established a detailed manual for IT budget formulation policy and procedures.
2. MCC establishes a budget for IT projects. A quarterly budget review is performed to refine budgeting requirements based on the status of projects and changing priorities.
3. MCC has documented a decision-making process to prioritize the allocation of IT resources.

Opportunities for Improvement

1. The MCC budget process recently changed from line item budgeting to project budgeting (i.e., balance sheet line item vs. MIDAS project), however the budget policy and procedures manual does not reflect this change.
2. There is not a clear line of site between the IT budget and project tracking to determine earned value.
3. The decision-making process to prioritize the allocation of IT resources is not consistently applied. A process for determining the priority for projects established by the business units has not been established.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 3 – Defined

COBIT Definition - Policies and processes for investment and budgeting are defined, documented and communicated, and cover key business and technology issues. The IT budget is aligned with the strategic IT and business plans. The budgeting and IT investment selection processes are formalized, documented and communicated. Formal training is emerging but is still based primarily on individual initiatives. Formal approval of IT investment selections and budgets is taking place. IT staff members have the expertise and skills necessary to develop the IT budget and recommend appropriate IT investments.

Recommendations

8. We recommend that the Millennium Challenge Corporation Deputy Chief Financial Officer revise the budget policy and procedures to account for the change from line item budgeting to project budgeting.

9. We recommend that the Millennium Challenge Corporation Chief Information Officer develop a process and implement a tool for monitoring project plans and work completed to determine earned value, providing an early warning of performance issues impacting project budgets.

Suggestions

4. We suggest that the Millennium Challenge Corporation Chief Information Officer develop a process to consistently implement the decision-making process to prioritize the allocation of Information Technology resources.

COBIT PO8 - Manage Quality

Observed Best Practices

1. MCC utilizes quality satisfaction surveying which results in improvement actions to address issues.

Opportunities for Improvement

1. A Quality Management System (QMS) that identifies quality requirements and criteria, and monitors performance against these requirements and criteria for continuous improvement of IT services is not in place.

2. Standards, procedures, and practices for key IT processes have not been identified and documented. Key IT processes include development and acquisitions that follow the life cycle of the deliverable.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 1 – Initial/Ad Hoc

COBIT Definition - There is a management awareness of the need for a QMS. The QMS is driven by individuals where it takes place. Management makes informal judgments on quality.

Recommendations

10. We recommend that the MCC Chief Information Officer (CIO) define quality requirements, criteria and key performance indicators for evaluation of quality management for key Information Technology processes.

11. We recommend that the MCC Chief Information Officer (CIO) identify and document standards, procedures, and practices for key Information Technology processes to guide the Agency in defining and evaluating criteria for quality management.

COBIT PO10 - Manage Projects

Observed Best Practices

1. MCC utilizes a portfolio tracker to track the status of major IT projects.

2. MCC requires project managers to obtain project management certification.

Opportunities for Improvement

1. MCC does not consistently apply formalized project management practices for all IT projects. Examples include:

    a. The project governance structure does not establish elements such as a project office, project manager, and project sponsors for all projects;

    b. The project management approach does not identify key criteria in which project performance may be measured;

    c. Project stakeholders are not required to ascertain whether the project delivered the planned results and benefits;

    d. The initiation of each major project phase is inconsistently approved, which may result in the lack of review or acceptance of deliverables in the previous phases;

    e. The responsibilities, authorities, and performance criteria of project members are not defined.

    f. Lessons learned are not documented for use on future projects and programs

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 2 – Repeatable but Intuitive

COBIT Definition - Senior management gains and communicates an awareness of the need for IT project management. The organization is in the process of developing and utilizing some techniques and methods from project to project. IT projects have informally defined business and technical objectives. There is limited stakeholder involvement in IT project management. Initial guidelines are developed for many aspects of project management. Application of project management guidelines is left to the discretion of the individual project manager.

Recommendations

12. We recommend that the Millennium Challenge Corporation Chief Information Officer implement a process to incorporate the following components into its projects:

    a. A project governance structure that includes the roles, responsibilities, and accountabilities of various key players in project management.

    b. Project sponsors assigned for the execution of each project.

c. Project office and project manager.

d. Elements such as approving the initiation of phases, communicating to all stakeholders the status of projects, establishing an integrated project plan, project quality plan, and defining the responsibilities of project team members.

e. Project risk management through the process of planning, identifying, analyzing, responding to, monitoring and controlling risk.

f. Project change control.

g. Lessons learned.

Acquire and Implement (AI)

Acquiring Application Software and Technology Infrastructure

MCC has drafted a System Development Life Cycle (SDLC) plan to guide development projects and help ensure the applications developed meet desired business needs. However, the SDLC has not been implemented. The SDLC Implementation Guide includes roles and responsibilities and describes each of the phases of the system development lifecycle including: Initiation, System Concept Development, Planning, Requirements, Design, Development, Integration and Test, Implementation, Operations and Maintenance, and Disposition. The SDLC methodology will be used for all major information technology development projects which have been defined in legislation as meeting one or more of the following: (1) the estimated total cost of development equals or exceeds $1 million; (2) the project is undertaken to support a critical business function; or (3) the Enterprise Architecture Steering Committee/CIO determines that the project requires the special attention and consideration given to a major information technology development project. For other changes to the MCC IT environment, including software and hardware, review and approval is required by the MCC Change Control Board (CCB). The CCB approval process is designed for acquisitions less than $300,000, and is typically for non-standard software requirements requested by users. Applications and projects of a higher cost are managed by the Enterprise Architecture Steering Committee (EASC). Per the EASC Charter, the EASC is responsible for establishing project managers and business sponsors for all major information technology investments above a $300,000 threshold. An Integrated Business Team (IPT) is responsible for defining business requirements and functions as well as detailed design documents, which are reviewed and approved by the EASC.

MCC addresses the initial risk management of procurements through the use of Risk Management Plans and Exhibit 300 business cases. However, these have not been consistently used, monitored and updated annually where procurements are occurring outside of the guidance of the Office of the Chief Information Officer. Although the SDLC Implementation Guide briefly discusses security and risk management, detailed policies and procedures regarding how application security, availability, and risks are managed when procuring an IT asset are not documented. In addition, MCC has not developed and implemented a policy to address the need to automate controls in procured software.

Acquisition, implementation and maintenance of the technological infrastructure are not consistently in line with the established functional and technical requirements due to the IT Strategic Plan not being updated to align with MCC's strategy. MCC completed a *Tool Gap Analysis and Strategy Plan* to determine whether Enterprise Content Management (ECM) platforms and tools are meeting business requirements and performed benchmarking to determine the tools best suited for MCC. The tools and applications reviewed were those specifically designed and used for Content Management (CM), Business Process Management (BPM), and Records Management (RM). The outcome of the analysis pinpointed gaps where the current ECM tools are not aligned with business requirements. This information will be used to establish the course of action necessary to align the required business tools with Enterprise Architecture efforts.

Installing and Accrediting Solutions

The Agency currently ensures that newly acquired systems are accredited and performs evaluations of implemented systems through Independent Verification & Validation Assessments (IV&V). For example, MCC completed a post production review of MCC's Integrated Data Analysis System (MIDAS), launched in March 2009, through an IV&V. However, there were several issues noted related to integration, testing and installation of new systems. MCC has not documented policies and procedures for data conversion, testing of applications, and infrastructure migration of new systems. Integration of acquired software is not always considered and planned during design and testing phases. In addition, MCC has not consistently evaluated whether user requirements have been met and personnel are not adequately trained in the use of developed applications. This has led to systems, such as MIDAS, entering production that are unsatisfactory to users and require additional cost and support to function within the technology infrastructure.

Application and Technology Infrastructure Maintenance

Maintenance and security of the technological infrastructure is outsourced to contractors as a cost saving measure. The contracts in place include performance metrics for maintaining the patching program. MCC has also implemented infrastructure vulnerability scanning to assist with patch management. However, MCC does not currently have a strategy in place to fully address the maintenance of software applications. IT has not been involved in the project management of all software applications to ensure that software maintenance was considered in the long term application strategy. The SDLC Implementation Guide describes the operations and maintenance phase of the software development life cycle; however, detailed policies and procedures have not been documented.

Procuring IT Resources

The agency relies largely on contractors for systems development projects. Many of the issues previously discussed related to installing systems were due to contractors not meeting contractual obligations such as testing and end user training. These problems may be prevented if performance monitoring of contracts is consistently occurring. Procedures for establishing, modifying, and terminating contracts for suppliers are documented in the Contracting Operations Manual (COM), which is MCC's interpretation of the Federal Acquisition Regulations (FAR). Specifically, the COM provides clarifying language or interpretation of the FAR where further definition is required or where variations are required to meet the needs of MCC. Components of the COM include legal review, performance monitoring, security and debarment, suspension and ineligibility of contracts. The agency utilizes a Technical Evaluation Panel to ensure best fit based on specified requirements. Although the FAR and COM are utilized to guide IT acquisition, MCC does not have a formalized process in place to evaluate that all components of IT acquisition have been considered. For example, performance metrics, intellectual Property considerations, and contractual requirements are not consistently discussed during the IT acquisition process. Additionally, there is no process in place to ensure compliance with the policies and procedures such as post award and ongoing contract compliance reviews.

The summary of observations identified in the review as well as the assessed COBIT Maturity Level Ranking and recommendations are provided as follows:

COBIT AI2 - Acquire and Maintain Application Software

Observed Best Practices

1. A Change Control Board (CCB) monitors applications, including software and hardware changes. The approval process is designed for applications that are less than $300K and are typically for non-standard software requirements requested by users.

2. An Enterprise Architecture Steering Committee (EASC) manages higher cost Information Technology projects. Per the Charter, the EASC is "charged with establishing both project managers and business sponsors of all major Information Technology investments above a $300,000 threshold."

3. MCC has drafted a Software Development Life Cycle (SDLC) to guide its development projects that will help ensure that the applications developed meet desired business needs.

Opportunities for Improvement

1. Risk management plans and Exhibit 300 business cases are not consistently used and monitored where procurements are occurring outside of the Office of the Chief Information Officer.

2. MCC has not implemented the documented System Development Life Cycle (SDLC).

3. MCC has not addressed the need to automate controls in procured software.

4. The agency does not have a policy for how application security, availability, and risks are managed when procuring an IT asset.

5. MCC does not have a strategy in place to fully address the maintenance of software applications.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 1 – Initial/Ad Hoc

COBIT Definition - There is an awareness that a process for acquiring and maintaining applications is required. Approaches to acquiring and maintaining application software vary from project to project. Some individual solutions to particular business requirements are likely to have been acquired independently, resulting in inefficiencies with maintenance and support.

Recommendations

13. We recommend that the Millennium Challenge Corporation Chief Information Officer implement a process to verify that risk management plans and Exhibit 300 business cases are consistently used, monitored and updated annually for all Information Technology projects as required.

14. We recommend that the Millennium Challenge Corporation Chief Information Officer finalize and implement the System Development Life Cycle.

15. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a policy to fully address the maintenance of software applications.

Suggestions

5. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a policy to address the need to automate controls in procured software.

6. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a policy for managing application security, availability, and risks when procuring an Information Technology Asset.

COBIT AI3 - Acquire and Maintain Technology Infrastructure

Observed Best Practices

1. MCC outsources the management of infrastructure and security components as a cost saving measure.

2. MCC has implemented infrastructure vulnerability scanning to assist with patch management.

3. MCC completed a *Tool Gap Analysis and Strategy Plan* to determine whether platforms and tools are meeting business requirements and performed benchmarking to determine the tools best suited for MCC.

Opportunities for Improvement

1. Integration of software into the current infrastructure is not consistently regarded in design or testing.

2. Acquisition, implementation and maintenance of the technological infrastructure is not consistently in line with the established business functional and technical requirements.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 2 – Repeatable but Intuitive

COBIT Definition - There is a consistency among tactical approaches when acquiring and maintaining the IT infrastructure. Acquisition and maintenance of IT infrastructure are not based on any defined strategy and do not consider the needs of the business applications that must be supported. There is an understanding that the IT infrastructure is important, supported by some formal practices. Some maintenance is scheduled, but it is not fully scheduled and co-ordinated. For some environments, a separate test environment exists.

Recommendations

16. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process for ensuring the integration of software into the current infrastructure is properly planned and executed.

Suggestions

7. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a plan for aligning the acquisition, implementation and maintenance of the technological infrastructure with business requirements as defined by the revised Information Technology Strategic Plan.

COBIT AI5 - Procure IT Resources

Observed Best Practices

1. Procedures exist for establishing, modifying, and terminating contracts for suppliers. Components include legal review, performance monitoring, security and debarment, suspension and ineligibility of contracts.

2. A Technical Evaluation Panel is used to establish a formal practice to ensure best fit for suppliers based on specified requirements.

Opportunities for Improvement

1. MCC has not formalized a process to evaluate that all components of IT acquisition (i.e., metrics, intellectual property considerations, contract requirements) have been addressed.

2. MCC does not have a process in place to ensure compliance with policies and procedures for IT Acquisition prior to reviews conducted by appropriate parties, such as the Legal Department, the Managing Director, etc.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 3 – Defined

COBIT Definition - Management institutes policies and procedures for IT acquisition. Policies and procedures are guided by the business organization's overall procurement process. IT acquisition is largely integrated with overall business procurement systems. IT standards for the acquisition of IT resources exist. Suppliers of IT resources are integrated into the organization's project management mechanisms from a contract management perspective. IT management communicates the need for appropriate acquisitions and contract management throughout the IT function.

Recommendations

17. We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement Information Technology Acquisition instructions that provide

a methodology to evaluate the components of Information Technology acquisition contracts.

Suggestions

8. We suggest that the Millennium Challenge Corporation Director of Contracting develop and implement a process for ensuring compliance with policies and procedures for Information Technology acquisition.

COBIT AI7 - Install and Accredit Solutions and Changes

Observed Best Practices

1. MCC ensures that developed systems are accredited.

2. MCC performed a post-production review of an IT investment through an Independent Verification and Validation Assessment.

Opportunities for Improvement

1. MCC has not consistently implemented a standardized and measurable approach for evaluating whether user requirements have been met, which may lead to systems entering production that are unsatisfactory to users and management.

2. MCC has not ensured that personnel are trained in the use of developed applications.

3. MCC does not have documented policies and procedures for data conversion, testing of applications, and infrastructure migration.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 2 – Repeatable but Intuitive

COBIT Definition - There is some consistency amongst the testing and accreditation approaches, but typically they are not based on any methodology. The individual development teams normally decide the testing approach, and there is usually an absence of integration testing. There is an informal approval process.

Recommendations

18. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process to ensure end user testing and evaluation of developed applications.

19. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process to ensure personnel are trained in the use of developed applications.

20. We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement policies and procedures for data conversion, testing of applications and infrastructure migration.

Deliver and Support (DS)

Defining and Managing Third Party Services

A risk management strategy to identify and monitor information service providers is applied. Business requirements have been established and are used to determine whether skills are needed through contracting services. As such, MCC has categorized all critical information system suppliers, and contracts are in place with each supplier. The contracts document roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers. A formal process for reviewing contracts with suppliers at pre-defined intervals, such as at invoicing and exercising of option years, has been implemented.

Within each IT services contract, business requirements are documented. In addition, service level agreements (SLAs) have been developed and defined for critical IT third party service providers. Monitoring of the SLAs has been implemented, with the exception of services provided for the MIDAS application. For one key contract, an award fee/bonus is available in addition to the fixed price schedule. In the case of nonperformed or unsatisfactory work, MCC may deduct from the vendor's invoice all amounts associated with such unsatisfactory or non-performed work or allow the contractor to re-perform the work within a reasonable period subject to the discretion of the Contracting Officer Technical Representative. For other vendors, MCC communicates issues and requests correction; however, there is no connection between service level agreement requirements and compensation. Additionally, MCC does not have formalized procedures for resolving contractor performance shortfalls as was evident with the MIDAS project. Implementing periodic review and feedback of performance for all contractors should improve service delivery and support early detection of potential problems.

Managing Problems

Tier-one support is provided through a third-party organization, CSC, and we noted that a process is in place for reporting, classifying, tracking and remediating problems through this contract. A formal process is implemented to close problem records after successfully confirming the elimination of any known errors. Systems have been equipped with automatic detection or warning mechanisms which are continuously tracked and evaluated. In addition, bandwidth utilization and router availability are tracked and reported. Analysis is performed to determine the root cause of issues identified and monthly meetings are held with CSC senior management to discuss areas for improvement or efficiencies.

However, MCC has not evolved the problem management process into a proactive one that can anticipate and prevent problems or ensure that knowledge regarding patterns of past and future problems is maintained through regular communication with vendors and experts. Likewise, a means of producing continuous improvement based on analysis of problem management performance measures is not a mature practice yet.

The summary of observations identified in the review as well as the assessed COBIT Maturity Level Ranking and recommendations are provided as follows:

COBIT DS1 - Define and Manage Service Levels

Observed Best Practices

1. Business requirements have been established and are used to determine whether skills are needed through contracting services. Business requirements have been documented in each IT services contract.

2. Service levels have been developed and defined for critical IT services with some third party service providers.

Opportunities for Improvement

1. MCC does not have service level agreements for the contracts associated with MIDAS.

2. MCC does not have formalized procedures for resolving performance shortfalls of contractors.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 3 – Defined

COBIT Definition - Responsibilities are well defined, but with discretionary authority. The SLA development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to, but they may not address business needs.

Recommendations

21. We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement a process to enforce the creation of service level agreements for all endeavors requiring contract support.

Suggestions

9. We suggest that the Millennium Challenge Corporation Director of Contracting formalize procedures on resolving performance shortfalls of contractors.

COBIT DS2 - Manage Third Party Services

Observed Best Practices

1. All critical suppliers have been identified.

2. Contracts are in place with all suppliers.

3. Monitoring of SLAs with some third party service providers is implemented.

4. For one contract, defined reporting of service level achievement is linked to compensation.

5. Contracts with suppliers are reviewed at predefined intervals.

6. A risk management strategy is in place for all contracts.

Opportunities for Improvement

1. Defined reporting of service level achievement is not linked to compensation for all third-party service providers such as the services provided for the MIDAS application and for information security systems services.

2. Periodic review and feedback of performance is not implemented for all contractors to improve service delivery and support early detection of potential problems.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 4 – Managed and Measurable

COBIT Definition - Formal and standardized criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned. Vendor qualifications, risks and capabilities are verified on a continual basis. Service requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to assess current and future third-party services. Transfer pricing models are used in the procurement process. All parties involved are aware of service, cost and milestone expectations. Agreed-upon goals and metrics for the oversight of service providers exist.

Recommendations

22. We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement a process for periodic review and feedback of performance for all contractors to improve service delivery and support early detection of potential problems.

Suggestions

10. We suggest that the Millennium Challenge Corporation Director of Contracting verify that all contracts, prior to award include linkage of reporting of service level achievement to compensation. For contracts already in place, we recommend that MCC include linkage of reporting of service level achievment to compensation upon renewal.

COBIT DS10 - Manage Problems

Observed Best Practices

1. A process is in place for reporting, classifying, tracking and remediating problems through the CSC contract.

2. A process is in place for detecting system issues including warning mechanisms for early detection.

3. Analysis is performed to determine the root cause of issues identified and monthly meetings are held with CSC senior management to discuss areas for improvement or efficiencies.

Opportunities for Improvement

1. MCC has not evolved the problem management process into a proactive one that can anticipate and prevent problems.

2. MCC does not consistently maintain knowledge regarding patterns of past and future problems through regular contacts with vendors and experts.

3. MCC does not have a process in place to ensure continuous improvement based on analysis of problem management performance measures.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 4 – Managed and Measurable

COBIT Definition - The problem management process is understood at all levels within the organization. Responsibilities and ownership are clear and established. Methods and procedures are documented, communicated and measured for effectiveness. The majority of problems are identified, recorded and reported, and resolution is initiated. Knowledge and expertise are cultivated, maintained and developed to higher levels, as the function is viewed as an asset and major contributor to the achievement of IT objectives and improvement of IT services. Problem management is well integrated with interrelated processes, such as incident, change, availability and configuration management, and assists customers in managing data, facilities and operations. Goals and metrics have been agreed upon for the problem management process.

Suggestions

11. We suggest that the Millennium Challenge Corporation Chief Information Officer evaluate and update the problem management process to include processes for proactively anticipating and preventing future problems.

12. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a formal process for maintaining knowledge regarding patterns of past and future problems affecting the Agency through regular contacts with vendors and experts.

13. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a continuous improvement process based on analysis of problem management performance measures.

Monitor and Evaluate (ME)

Monitoring and Evaluating Performance

MCC has established the Enterprise Architecture Steering Committee (EASC) for monitoring large IT investment projects above a $300,000 threshold and utlizes a portfolio tracker to track the status of major IT projects. However, all IT projects and processes have not been regularly monitored by OCIO due to the reporting structure of the CIO which has, in the past, given priority to projects sponsored by the CFO, rather than ensuring all IT projects are provided a priority level commensurate with the direction and goals of the Agency as a whole. Recently, however the CIO has implemented a process for monitoring projects by assigning a project manager to all IT projects.

In addition, IT Risk Management Plans and Business Cases for IT projects in the form of Exhibit 300s are not consistently used to set performance targets. The Exhibit 300 requires documentation of the agency's mission, strategic goals, and performance measures (indicators). On the other hand, OCIO has implemented and is monitoring performance targets with the business in the form of the Service Level Agreements (SLAs) documented in the CSC contract. Monitoring these SLAs provides a measurement of how well the information services function is contributing to the performance of the organization.

Ensuring Compliance with External Requirements

MCC OCIO has processes in place to identify applicable laws and regulations that must be complied with for incorporation into the IT policies, standards, procedures and methodologies. With regard to information security, OCIO has a process in place to assist with ensuring compliance with the Federal Information Security Management Act (FISMA). With respect to managing IT investment projects, individuals charged with managing projects or contracts are required to have project management certificates or certifications for Contracting Officer Technical Representative (COTR) as specified by the Office of Management and Budget (OMB). Concerning acquisitions of IT resources and investments, MCC follows the Federal Acquisition Regulations (FAR). However, MCC does not have a process in place to monitor compliance with external requirements to ensure consistency. In addition, MCC does not have a process in place to review and adjust policies to ensure they comply with external requirements. For example, MCC does not have policies for adapting the FAR Part 39, *Acquisition of Information Technology*, to the Agency including assessing, monitoring and controlling risk when selecting projects for investment and during program implementation. Developing and implementing a program management office with oversight over compliance issues may assist the MCC OCIO in ensuring compliance with regulatory requirements and compliance with internal policies and procedures.

Providing IT Governance

The Enterprise Architecture Steering Committee (EASC) is a governance body that is in place to provide strategic direction to management relative to information Technology investments and the MCC CIO regularly reports to senior management regarding the progress of IT projects. IT project risk is initially assessed and documented through the use of Exhibit 300s. However, risk assessments for IT projects are inconsistently performed and there is no process in place for continuous monitoring of project risk, including the annual update of the Exhibit 300, as required by the Office of Management

and Budget (OMB). In addition to the EASC, governance over IT processes is also achieved through audits and reviews performed by the Office of Inspector General (OIG).

MCC has developed baseline IT Governance indicators in the IT Strategic Plan, for example establishing the Enterprise Architecture Steering Committee, maintaining FISMA compliance, and completing and approving risk assessments and OMB Exhibit 300s for IT projects. Although baseline governance indicators have been developed, a process has not been implemented for monitoring and reporting on key governance performance indicators leading to enterprise improvements.

The summary of observations identified in the review as well as the assessed COBIT Maturity Level Ranking and recommendations are provided as follows:

COBIT ME1 - Monitor and Evaluate Performance

Observed Best Practices

1. MCC has established an Enterprise Architecture Steering Committee for monitoring IT projects above a $300,000 threshold with senior management involvement and utlizes a portfolio tracker to track status of major IT projects.
2. MCC has established performance targets within the business and is monitoring those targets on a monthly basis.

Opportunities for Improvement

1. IT Risk Management Plans and Business Cases for IT projects are not consistently used to set performance targets.
2. All IT projects and processes had not been regularly monitored by OCIO due to the reporting structure of the CIO which had and could continue to give priority to projects sponsored by the CFO.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 3 – Defined

COBIT Definition - Management communicates and institutes standard monitoring processes. Educational and training programs for monitoring are implemented. A formalized knowledge base of historical performance information is developed. Assessment is still performed at the individual IT process and project level and is not integrated amongst all processes. Tools for monitoring IT processes and service levels are defined. Measurements of the contribution of the information services function to the performance of the organization are defined, using traditional financial and operational criteria. IT-specific performance measurements, non-financial measurements, strategic measurements, customer satisfaction measurements and service levels are defined. A framework is defined for measuring performance.

Recommendations

23. We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a monitoring process to ensure that all Information Technology projects are provided a priority level commensurate with the direction

and goals of the Agency as a whole, not with the goals of individual leaders within the Agency.

Suggestions

14. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a review process to verify the use of Information Technology Risk Management Plans and Business cases to ensure that performance targets are established for each Information Technology project.

COBIT ME3 - Ensure Compliance with External Requirements

Observed Best Practices

1. MCC identifies the external laws and requirements that must be complied with on a continuous basis.
2. MCC has implemented a process to assist in ensuring compliance with the Federal Information Security Management Act (FISMA).
3. MCC follows federal guidelines, the Federal Acquisition Regulations (FAR), for acquisitions.
4. Individuals charged with managing projects or contracts are required to have project management certificates or certifications for Contracting Officer Technical Representative as specified by the Office of Management and Budget (OMB).

Opportunities for Improvement

1. MCC does not have a process in place to review and adjust policies to ensure they comply with external requirements.
2. There is no program management office to monitor compliance with external requirements.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 4 – Managed and Measureable

COBIT Definition - Issues and exposures from external requirements and the need to ensure compliance at all levels are fully understood. A formal training scheme is in place to ensure that all staff members are aware of their compliance obligations. Responsibilities are clear and process ownership is understood. The process includes a review of the environment to identify external requirements and ongoing changes. There is a mechanism in place to monitor non-compliance with external requirements, enforce internal practices and implement corrective action. Non-compliance issues are analyzed for root causes in a standard manner, with the objective to identify sustainable solutions. Standardized internal good practices are utilized for specific needs, such as standing regulations and recurring service contracts.

Suggestions

15. We suggest that the Millennium Challenge Corporation Director of Contracting in collaboration with the Chief Information Officer develop and implement a process to review and adjust policies on a regular basis to ensure they comply with external requirements.

16. We suggest that the Millennium Challenge Corporation Chief Information Officer and the MCC Director of Contracting develop and implement a program management program to monitor compliance with external requirements.

COBIT ME4 - Provide IT Governance

Observed Best Practices

1. MCC obtains independent assurance of its IT environment through audits and reviews by the Office of Inspector General (OIG).
2. The Chief Information Officer regularly reports to senior management regarding the progress of IT projects.
3. A governance body (Enterprise Architecture Steering Committee) is in place to provide strategic direction to management relative to IT.
4. IT project risk is initially assessed and documented through the use of Exhibit 300s.
5. MCC has developed baseline IT Governance indicators in the IT Strategic Plan, for example establishing the Enterprise Architecture Steering Committee, maintaining FISMA compliance, and completing and approving risk assessments and OMB Exhibit 300s for IT projects.

Opportunities for Improvement

1. Risk assessments for IT projects are inconsistently performed and there is no process in place for continuous monitoring of project risk, including the annual update of the Exhibit 300, as required by the Office of Management and Budget (OMB).
2. Although baseline governance indicators have been developed a process has not been implemented for the monitoring and reporting on performance indicators leading to enterprise improvements.

Maturity Level Ranking and Definition as Defined by COBIT

Maturity Level: 2 – Repeatable but Intuitive

COBIT Definition - There is awareness of IT governance issues. IT governance activities and performance indicators, which include IT planning, delivery and monitoring processes, are under development. Selected IT processes are identified for improvement based on individuals' decisions. Management identifies basic IT governance measurements and assessment methods and techniques; however the process is not adopted across the organization. Communication on governance standards and responsibilities is left to the individual. Individuals drive the governance

processes within various IT projects and processes. The processes, tools and metrics to measure IT governance are limited and may not be used to their full capacity due to a lack of expertise in their functionality.

Recommendations

See Recommendation 13

Suggestions

17. We suggest that the Millennium Challenge Corporation Chief Information Officer develop and implement a process for monitoring and reporting on baseline performance indicators to assist with continuous process improvement.

RISK ASSESSMENT CONCLUSION

As MCC continues to select and manage its information technology investments, it is important to have a formal process in place to manage risk. This will assist in ensuring IT objectives are correlated with business objectives and IT investments are prioritized and managed to effectively support Agency initiatives. To address control gaps identified in MCC's IT governance over its information technology investments, MCC must carry out corrective actions to address the recommendations made in this report. In addition, MCC should consider the suggestions identified and determine a course of action for prioritizing and implementing the suggestions deemed appropriate according to a feasible timetable.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, Millennium Challenge Corporation (MCC) noted corrections should be made to pages five and ten of the draft report regarding references to the Chief Information Officer's (CIO) reporting relationship to MCC's Chief Executive Officer. Subsequent to the delivery of the draft Risk Assessment, the Office of Inspector General (OIG) informed MCC that the CIO's reporting relationship was no longer an open recommendation and that the OIG recognized that MCC made a management decision on this issue. Based on this information, modifications have been made to the report to reflect the closure of the previous recommendation. We have left the statement in the report because the risk was identified during our field work and the closure of the finding was not reported until after delivery of the draft report. Additionally, since a determination on the effectiveness of the new reporting structure has not been made, we still view this as a risk.

MCC also noted that a correction should be made regarding the completion date for the Enterprise Architecture Data Reference Module. In our draft, we reported a completion date of Spring 2011. Per management's response, the Data Reference Model will not be complete until September 2011. As a result, we have updated the report to reflect the correct completion date.

MCC management concurred with and agreed to take corrective action for each of the 23 recommendations. However, timelines for completion have been provided for only three of the recommendations. CG agrees with MCC's management decisions on those three recommendations, discussed below.

- For recommendation 17, management agreed to develop and implement IT acquisition instructions to include a methodology for acquisition planning that addresses the different components of IT acquisition contracts. The target completion to fully close this recommendation is July 31, 2011.

- For recommendation 21, management agreed to develop guidelines for establishing service level agreements and requirements for including those agreements in large and complex information technology contracts. The target completion to fully close this recommendation is July 31, 2011.

- For recommendation 22, management agreed to develop guidance and requirements for periodic contractor performance reviews that will provide for early detection of problems and improved service delivery on large and complex information technology contracts, including the use of the Contract Performance Assessment Rating System. The target completion to fully close this recommendation is July 31, 2011.

For the remaining recommendations, MCC management plans to prepare a Combined Corrective Action Plan by July 31, 2011. MCC management indicated that the plan will address the milestones and dates associated with the remaining recommendations. MCC's management comments are included in their entirety in Appendix II.

SCOPE AND METHODOLOGY

Scope

The risk assessment was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. In addition, our work in support of the risk assessment was guided by Information Technology Governance Institute's Control Objectives for Information and related Technology (COBIT) framework version 4.1. COBIT provides managers, auditors and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of IT and developing appropriate IT governance and control in an organization. It provides good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by bridging the gaps between business risks, technical issues, control needs and performance measurement requirements.

In the absence of specific federal guidance solely focused on governance over IT investments, we believe Information Technology Governance Institute's COBIT provides best practices in helping organizations assess their governance controls. However, since MCC must comply with federal laws and regulations, we mapped COBIT 4.1 to National Institute of Standards and Technology (NIST) 800-53 Rev 3 controls, where applicable. See Appendix IV.

We conducted our audit at the Millennium Challenge Corporation (MCC) Headquarters in Washington, DC, from October 11, 2010, to January 27, 2011. To answer the assessment objective, we conducted interviews with MCC staff and reviewed documentation related to IT governance processes and control objectives under evaluation. Such documentation included the *MCC IT Strategic Plan*, the *September 2010 CIO Brief to the MCC Vice President*, the *Enterprise Architecture Steering Committee Charter* and meeting minutes, the *IT Project Budget*, the *OCIO 2-Year Portfolio of IT projects*, the OCIO Portfolio Tracking Dashboard, contracts and service level agreements for service providers, the *Contracting Operations Manual* (COM), the *Exhibit 300: Capital Asset Plan and Business Case Summary for the MIDAS application*, the current and proposed CIO organizational structure, and the CIO IT Operational Budget Benchmarking Report. We reviewed laws, regulations, OMB circulars and memorandums, and other guidance related to the assessment objective. The objective of this assessment was to determine what MCC's risks are for selecting, managing, and controlling its information technology investments. The IT investments reviewed included MCC Integrated Data Analysis System (known as MIDAS), Integrated Financial and Contract Management System (IFCMS), Enterprise Content Management (ECM), and additional support contracts.

We reviewed laws, regulations, OMB circulars and memorandums, and other guidance related to the assessment objective. The assessment did not include risks with respect to security and privacy.

Methodology

Our methodology was categorized into three phases: the planning, testing (fieldwork),

and reporting phases. The primary objective of the planning phase was to develop the audit program and the work plan that addressed the tasks outlined in the Statement of Work. The primary objective of the testing phase was to assist the MCC AIG in assessing the risk assessment areas as defined below and complete the risk assessment procedures as defined in the audit program. Specifically, we:

- Evaluated and tested selected IT processes and control objectives for MCC (described in the Control Objectives for Information and related Technology (COBIT) framework version 4.1);
- Interviewed key personnel and obtained and examined documentation related to the IT processes and control objectives under review; and
- Assigned a maturity level to each IT process evaluated, which range from non-existent (0) to optimized (5).

The risk assessment methodology utilized the COBIT version 4.1, which provides a mechanism for measuring how well developed management processes are in relation to accepted industry standards. The use of COBIT's maturity model assisted us in measuring performance and addressing gaps in capability in assessing the effectiveness of MCC's IT governance practices over its IT investments.

The key COBIT IT governance areas we focused on are:

IT Governance Area	Definition	Importance	Standard/Best Practice
Plan and Organize			
Define a Strategic IT Plan	Creating a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks	Incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner	COBIT PO1
Define the Information Architecture (MCC's enterprise architecture)	Creating and regularly updating a business information model and defining the appropriate systems to optimize the use of this information	Being agile in responding to requirements, to provide reliable and consistent information and to seamlessly integrate applications into business processes	COBIT PO2
Define the IT Processes, Organization and Relationships (IT governance committees)	Establishing transparent, flexible and responsive IT organizational structures and defining and implementing IT processes with owners, and roles and responsibilities integrated into business and decision	Being agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact	COBIT PO4

IT Governance Area	Definition	Importance	Standard/Best Practice
	processes		
Manage the IT Investment	Establishing effective and efficient IT investment and portfolio decisions, and setting and tracking IT budgets in line with IT strategy and investment decisions	Improving IT's cost-efficiency and its contribution to business profitability with integrated and standardized services that satisfy end-user expectations	COBIT PO5
Manage Quality	Establishing effective ongoing performance monitoring against predefined objectives and implementing a program for continuous improvement of IT services	Ensuring continuous and measurable improvement of the quality of IT services delivered.	COBIT PO8
Manage Projects	Defining a program and project management approach that is applied to IT projects and enables stakeholder participation in and monitoring of project risks and progress	Ensuring the delivery of project results within agreed-upon time frames, budget and quality	COBIT PO10
Acquire and Implement			
Acquire and Maintain Application Software	Ensuring that there is a timely and cost-effective development process	Aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost	COBIT AI2
Acquire and Maintain Technology Infrastructure	Providing appropriate platforms for the business applications in line with the defined IT architecture and technology standards	Acquiring and maintaining an integrated and standardized IT infrastructure	COBIT AI3
Procure IT Resources	Acquiring and maintaining IT skills that respond to the IT strategy, integrating and standardizing IT infrastructure, and reducing IT procurement risk	Improving IT's cost-efficiency and its contribution to business profitability	COBIT AI5
Install and Accredit Solutions and Changes	Testing that applications and infrastructure solutions are fit for the intended purpose and free from errors, and planning releases to	Implementing new or changed systems that work without major problems after installation	COBIT AI7

IT Governance Area	Definition	Importance	Standard/Best Practice
	production		
Deliver and Support			
Define and Manage Service Levels	Identifying service requirements, agreeing on service levels and monitoring achievement of service levels	Ensuring the alignment of key IT services with the business strategy	COBIT DS1
Manage Third-party Services	Establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements	Providing satisfactory third-party services while being transparent about benefits, costs and risks	DS2
Manage Problems	Recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems	Ensuring end users' satisfaction with service offerings and service levels, and reducing solution and service delivery defects and rework	COBIT DS10
Monitor and Evaluate			
Monitor and Evaluate IT Performance	Monitoring and reporting process metrics and identifying and implementing performance improvement actions	Transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements	COBIT ME1
Ensure Compliance with External Requirements	Identifying all applicable laws, regulations and contracts and the corresponding level of IT compliance and optimizing IT processes to reduce the risk of non-compliance	Ensuring compliance with laws, regulations and contractual requirements	COBIT ME3
Provide IT Governance	Preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions	Integrating IT governance with corporate governance objectives	COBIT ME4

The COBIT maturity model is based on evaluating and rating an organization on maturity levels of non-existent (0) to optimized (5).

We performed a process maturity evaluation using the following COBIT maturity levels:

0 **Non-Existent:** There is a complete lack of any recognizable processes. The organization has not even recognized there is an issue to be addressed.

1 **Initial/Ad hoc:** There is evidence that the organization has recognized that issues exist and need to be addressed. There are, however, no standardized processes, but instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

2 **Repeatable but Intuitive:** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals, and therefore, errors are likely.

3 **Defined Process:** Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices.

4 **Managed and Measureable:** Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 **Optimized:** Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

The COBIT maturity model for each IT governance area assessed is included in Appendix III.

MANAGEMENT COMMENTS

April 29, 2011

To: Alvin Brown
Office of Inspector General
Millennium Challenge Corporation

From: Dennis Lauer, CIO /s/
Millennium Challenge Corporation
875 Fifteenth Street NW
Washington, DC 20005

REF: MCC Request for extension and notice of final action memorandum dated *3/25/2011*

Subject: MCC Combined Management Response for the MCC's Implementation of Selected Key Project Controls for the MCC Integrated Data Analysis System (MIDAS) (M-000-11-002-P) and draft Risk Assessment of MCC's Information Technology (IT) Governance over its IT Investments (M-000-11-00X-P)

Dear Mr. Brown:

The Millennium Challenge Corporation (MCC) appreciates the opportunity to further address the audit of MCC's Implementation of Selected Key Project Controls for MIDAS and the draft Risk Assessment of MCC's Information Technology Governance over its IT Investments.

Before addressing the specific recommendations in the Risk Assessment, MCC notes that corrections should be made to pages five and ten of the draft report regarding references to the Chief Information Officer's (CIO) reporting relationship to MCC's Chief Executive Officer (CEO). Specifically, these references state that the CIO's dotted line reporting relationship to the CEO does not reflect the level of importance of IT issues within MCC. Subsequent to the issuance of this draft Risk Assessment, the Office of Inspector General (OIG) informed MCC that the CIO's reporting relationship was no longer an open recommendation and that the OIG recognized that MCC made a management decision on this issue. The OIG reserved the right to monitor the issue in future IT audits, but the

circumstances outlined in the MIDAS and IT governance audits predate the reporting relationship change implemented by MCC. A copy of the OIG memorandum is attached.

MCC understands and appreciates the important role of proper IT governance to ensure that IT investments are aligned and prioritized within corporate business objectives and available corporate resources. Effective management is critical to deliver projects on schedule and within budget, as well as to assure that projects meet their objective. Considering that MCC has only operated for seven years, the Agency already has made significant progress toward establishing effective governance of IT investrnents. Specifically, a few of the steps already taken to implement IT governance rigor at MCC are:

1. Established a comprehensive IT Governance structure including the Enterprise Architecture Steering Committee (EASC), a newly established Executive Advisory Board (EAB), Integrated Project Teams (IPTs) and working groups for the major IT project(s).

2. Revised the EASC charter to reflect the new structure.

3. Established a charter for the MIDAS Integrated Project Team.

4. Established weekly project reviews by the CIO with each project manager.

5. Developed two tools (the Executive Level tracker and the PM central task manager) to manage budget, schedule and risk for IT investments.

6. Established and filled a dedicated Program Manager position to develop and manage the Combined Corrective Action Plan (CCAP).

7. Awarded a multi-year IT Planning contract to provide the incremental technical support required to execute the corrective action plan.

While MCC concurs with the 23 IT Governance recommendations and the 9 MIDAS audit recommendations, it became apparent that we needed more time to develop a detailed CCAP. Consistent with the principles emphasized in the recommendations on good governance thorough advance planning, realistic timeframes, and the identification of requisite resources, MCC is ensuring that the CCAP itself reflects solid project management. As part of this effort MCC will review the plan with the EASC, identify resource requirements, and allocate budgetary and other resources to develop and execute our corrective action plan. The current budget environment and rational sequencing of the combined 32 recommendations will require MCC to prioritize and divide into implementation phases the deliverables within the action plan.

Therefore, MCC will develop a CCAP by July 31, 2011. The CCAP will address the recommendations contained in MCC'S Implementation of Selected Key Project Controls for MIDAS (M-000-ll-002-P) and the draft report on the Risk Assessment Of The Millennium Challenge Corporation's Information Technology Governance Over Its Information Technology Investments (M-000-ll-00X-P).

The CCAP will incorporate the recommendations from both documents into a cohesive approach and ensure the most effective use of MCC's resources. Budgetary projections indicate a constrained environment for the foreseeable future. As such, this CCAP will focus on the judicious use of limited funds to achieve the greatest impact toward maturing MCC's IT governance processes and structure. The basic structure and consolidation objectives of the MCC CCAP follow below.

The MCC CCAP will be divided into four phases. The first phase is the Systems Development Life Cycle (SDLC) policy and procedures development and roll-out, and it will address MIDAS recommendations 1, 5, 6, 7, 8, 9 and IT Governance recommendations 12, 14, 18, 19, 20, 23. The second phase is the planning and establishment of the policies and procedures for the MCC IT Program Management Office (PMO). This phase will address MIDAS recommendation 3 and IT Governance recommendations 1, 2, 5, 6, 7, 8, 13, 15, 16, 17, 21, 22. The third phase is the implementation of the PMO and will address MIDAS recommendation 2, 4 and IT Governance recommendations 9, 10, 11. The fourth phase is the evaluation and adjustment phase and it will address IT Governance recommendations 3 and 4.

CCAP Phase One:

MIDAS Recommendation No. 1: Develop a detailed, written plan to establish strong project management capabilities for IT projects.

Management Response: MCC will develop a CCAP to establish project management capabilities for Information Technology projects by July 31st, 2011.

MIDAS Recommendation No. 5: Develop written policies and procedures to obtain written approval for relying on a contractor's systems development life cycle (SDLC) methodology.

Management Response: MCC will establish a corporate SDLC policy. The milestones and dates associated with this deliverable will be addressed in the Combined Action Plan.

MIDAS Recommendation No. 6: Develop written policies and procedures to address key decision points for IT projects.

Management Response: MCC will develop SDLC procedures to address key decision points for Information Technology projects. The milestones and dates associated with this deliverable will be addressed in the Combined Action Plan.

MIDAS Recommendation No. 7: Establish in writing what documentation must be prepared, updated, and maintained for IT projects.

Management Response: MCC will develop SDLC procedures which will address the documentation necessary for maintaining IT projects. The milestones and dates associated with this deliverable will be addressed in the Combined Action Plan.

MIDAS Recommendation No. 8: Implement risk management, earned value management, and requirements management for the MIDAS project before proceeding to the development phase to build additional functionality for the system.

Management Response: MCC will implement risk management, earned value management and requirements management for the MIDAS project before proceeding to the development phase to build additional functionality for the system. The milestones and dates associated with this deliverable will be addressed in the CCAP. The current systems to manage risk, earned value, and requirements for the MIDAS project will be adjusted as necessary to meet the milestones and dates in the CCAP.

MIDAS Recommendation No. 9: Review MCC's IT project management capabilities and determine whether its weaknesses should be reported, tracked, and monitored as a material weakness pursuant to the Federal Managers Financial Integrity Act of 1982.

Management Response: MCC will refer this to the Senior Assessment Board (SAB) for a determination of whether IT project management capabilities should be reported, tracked and monitored as a material weakness pursuant to the Federal Managers Financial Integrity Act of 1982. The milestone and date associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 12: We recommend that the Millennium Challenge Corporation Chief Information Officer implement a process to incorporate the following components into its projects:

- A project governance structure that includes the roles, responsibilities, and accountabilities of various key players in project management.
- Project sponsors assigned for the execution of each project.
- Project office and project manager.
- Elements such as approving the initiation of phases, communicating to all stakeholders the status of projects, establishing an integrated project plan, project quality plan, and defining the responsibilities of project team members.
- Project risk management through the process of planning, identifying, analyzing, responding to, monitoring and controlling risk.
- Project change control.
- Lessons learned.

Management Response: MCC will incorporate these components into Information Technology (IT) projects with the implementation of a systems development life cycle. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 14: We recommend that the Millennium Challenge Corporation Chief Information Officer finalize and implement the system development life cycle.

Management Response: MCC's CIO will finalize and implement the SDLC. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 18: We recommend that the Millennium Challenge

Corporation Chief Information Officer develop and implement a process to ensure end user testing and evaluation of developed applications.

Management Response: MCC's CIO will develop and implement a process to ensure end user testing and evaluation of developed applications with the implementation of the systems development life cycle. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 19: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process to ensure personnel are trained in the use of developed applications.

Management Response: MCC's CIO will develop and implement a process to ensure personnel are trained in the use of developed applications with the implementation of the systems development life cycle. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 20: We recommend that the Millennium Challenge Corporation Chief Information Officer document and implement policies and procedures for data conversion, testing of applications and infrastructure migration.

Management Response: MCC's CIO will document and implement policies and procedures for data conversion, testing of applications and infrastructure migration with the implementation of the systems development life cycle. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 23: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a monitoring process to ensure that all IT projects are provided a priority level commensurate with the direction and goals of the Agency as a whole, not with the goals of individual leaders within the Agency.

Management Response: The MCC's CIO will develop and implement a monitoring process to ensure that all IT projects are included as part of the Enterprise IT portfolio review process. The milestones and dates associated with this deliverable will be addressed in the CCAP.

CCAP Phase Two:

MIDAS Recommendation No. 3: Develop written policies and procedures to plan for, mitigate, monitor, and report on risks to IT projects.

Management Response: MCC will develop an IT Project Risk Management Policy. The milestone and date associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 1: We recommend that the Millennium Challenge Corporation Chief Information Officer update the information technology strategic plan to reflect current enterprise strategic goals.

Management Response: MCC's CIO will update the information technology strategic plan to reflect current enterprise strategic goals. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 2: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a formal process for managing risk and updating the information technology strategic plan accordingly. Risk management must drive enterprise architecture decisions, providing secure information system environments for critical applications. The plan should be reviewed at a minimum annually and when major events occur that have an impact on strategic goals. When updating the information technology strategic plan the Chief Information Officer should verify compliance with the Office of Management and Budget Circular No. A-130, Management of Federal Information Systems, with regard to the capital planning and investment control process which includes the information resource management strategic plan and the information technology capital plan which is required to be updated twice yearly.

Management Response: The MCC's CIO will develop and implement a formal process for managing risk and updating the information technology strategic plan accordingly. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 5: We recommend that the Millennium Challenge Corporation Chief of Staff develop and implement a formal process that must be consistently applied for the Enterprise Architecture Steering Committee to prioritize information technology enabled-investment programs.

Management Response: The MCC's Chief of Staff (CoS) will develop, implement, and consistently apply a formal process for the EASC to prioritize information technology-enabled investment programs. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 6: We recommend that the Millennium Challenge Corporation Chief of Staff formally document and implement a process requiring the Enterprise Architecture Steering Committee to consider risk management when discussing strategic direction and approval of information technology investments.

Management Response: MCC's CoS will formally document and implement a process requiring the EASC to consider risk management when discussing strategic direction and approval of information technology investments. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 7: We recommend that Millennium Challenge Corporation Chief Information Officer (1) conduct an analysis to determine whether the information technology function has sufficient resources to adequately support the business goals and objectives of the organization and (2) through the organization's budgeting process, submit a written request for additional resources to address any shortfalls identified in the analysis.

Management Response: Within the context of MCC's overall budgetary constraints and budgeting process, MCC's CIO will (l) conduct an analysis to determine whether the information technology function has sufficient resources to adequately support the business goals and objectives of the organization and (2) through the organization's budgeting process, submit a written request for additional resources to address any shortfalls identified in the analysis. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 13: We recommend that the Millennium Challenge Corporation Chief Information Officer implement a process to verify that risk management plans and Exhibit 300 business cases are consistently used, monitored and updated annually for an IT projects as required.

Management Response: The MCC's CIO will implement a process to verify that risk management plans and Exhibit 300 business cases are consistently used, monitored and updated annually for all IT projects as required. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 15: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a policy to fully address the maintenance of software applications.

Management Response: MCC's CIO will develop and implement a policy to fully address the maintenance of software applications. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 16: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a process for ensuring the integration of software into the current infrastructure is properly planned and executed.

Management Response: MCC's CIO will develop and implement a process for ensuring the integration of software into the current infrastructure is properly planned and executed. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 8: We recommend that the Millennium Challenge Corporation Deputy Chief Financial Officer revise the budget policy and procedures to account for the change from line item budgeting to project budgeting.

Management Response: MCC's Deputy Chief Financial Officer will revise the budget and policy procedures to account for the change from the line item budgeting to project budgeting for Information Technology projects. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 17: We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement information technology acquisition instructions that provide a methodology to evaluate the components of information technology acquisition contracts.

Management Response: The MCC's Managing Director for Contracts and Grant Management (CGM) will develop and implement IT acquisition instructions to include a methodology for acquisition planning that addresses the different components of IT acquisition contracts by July 31, 2011.

IT Governance Recommendation No. 21: We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement a process to enforce the creation of service level agreements for all endeavors requiring contract support.

Management Response: MCC's Managing Director for CGM will develop guidelines for establishing SLAs and requirements for including SLAs in large and complex information technology contracts by July 31, 2011.

IT Governance Recommendation No. 22: We recommend that the Millennium Challenge Corporation Director of Contracting develop and implement a process for periodic review and feedback of performance for all contractors to improve service delivery and support early detection of potential problems.

Management Response: MCC's Managing Director for CGM will develop guidance and requirements for periodic contractor performance reviews that will provide for early detection of problems and improved service delivery on large and complex information technology contracts, including the use of the Contract Performance Assessment Rating System (CPARS,) by July 31, 2011.

CCAP Plan Phase Three:

MIDAS Recommendation No. 2: Develop written earned value management policies and procedures for IT projects, as required.

Management Response: MCC will develop an Earned Value Management policy that is ANSI-EIA 748A compliant. The milestones and dates associated with this deliverable will be addressed in the CCAP.

MIDAS Recommendation No .4: Update the Contracts Operating Manual to include procedures for including risk management and earned value management in contracting actions, when required.

Management Response: MCC will update the Contracts Operating Manual to include procedures for including risk management and earned value management in contracting actions, when required. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 9: We recommend that the Millennium Challenge Corporation Chief Information Officer develop a process and implement a tool for monitoring project plans and work completed to determine earned value, providing an early warning of performance issues impacting project budgets.

Management Response: MCC's CIO will develop a process and implement a tool for monitoring project plans and work completed to determine earned value, providing an early warning of performance issues impacting project budgets. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 10: We recommend that the Millennium Challenge Corporation Chief Information Officer define quality requirements, criteria, and key performance indicators for evaluation of quality management for key IT processes.

Management Response: The MCC's CIO will define quality requirements, criteria, and key performance indicators for evaluation of quality management for key IT processes. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 11: We recommend that the Millennium Challenge Corporation Chief Information Officer identify and document standards, procedures, and practices for key IT processes to guide the Agency in defining and evaluating criteria for quality management.

Management Response: MCC's CIO will identify and document standards, procedures, and practices for key IT processes to guide the Agency in defining and evaluating criteria for quality management. The milestones and dates associated with this deliverable will be addressed in the CCAP.

CCAP Phase Four:

IT Governance Recommendation No. 3: We recommend that the Millennium Challenge Corporation Chief Information Officer complete the enterprise information architecture planning and implementation project as discussed in the Executive Level Notional OCIO 2 Year Portfolio in order to maintain an information architecture that reflects the business requirements.

Management Response: MCC's CIO will complete the enterprise information architecture planning and implementation project as discussed in the Executive Level Notional OCIO 2 Year Portfolio in order to maintain an information architecture that reflects the business requirements. The milestones and dates associated with this deliverable will be addressed in the CCAP.

IT Governance Recommendation No. 4: We recommend that the Millennium Challenge Corporation Chief Information Officer develop and implement a project plan for leveraging data as indicated in the authoritative data source process and methodology in order to provide business users access to detailed information to aid in analysis and decision making by June 30th, 2012.

Management Response: MCC's CIO will develop and implement a project plan for leveraging data as indicated in the authoritative data source process and methodology in order to provide business users access to detailed information to aid in analysis and decision making. The milestones and dates associated with this deliverable will be addressed in the CCAP.

Finally, there are statements in the draft report on the Risk Assessment that should be clarified. The document indicates that the Enterprise Architecture Data Reference Model (DRM) would be complete in the Spring of 2011, whereas the DRM will not actually be complete until September 2011.

If you have any questions, comments or concerns please feel free to contact me on 202.521. 7257.

Attachments:

CC: IG/MCC, Lisa Banks
IG/MCC, Aleta Johnson
MCC/A&F/FMD, Arlene McDonald

COBIT MATURITY MODEL MEASURMENT CRITERIA

PO1 Define a Strategic IT Plan

PO 1 Maturity Model

Control over the IT process “Define a Strategic IT Plan” with the business goal of sustaining or extending the business strategy and governance requirement while remaining transparent about benefits, costs and risks.

Measurement

0 Non-existent when

IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial/Ad Hoc when

The need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement. IT strategic planning is occasionally discussed at IT management meetings. The alignment of business requirements, applications and technology takes place reactively rather than by an organization wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive when

IT strategic planning is shared with business management on an as-needed basis. Updating of the IT plans occurs in response to requests by management. Strategic decisions are driven on a project-by-project basis without consistency with an overall organization strategy. The risks and user benefits of major strategic decisions are recognized in an intuitive way.

3 Defined when

A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach that is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process, and there are no procedures to examine the process. The overall IT strategy includes a consistent definition of risks that the organization is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly influence the acquisition of new products and technologies. IT strategic planning is discussed at business management meetings.

4 Managed and Measurable when

IT strategic planning is standard practice and exceptions would be noticed by

management. IT strategic planning is a defined management function with senior-level responsibilities. Management is able to monitor the IT strategic planning process, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organization, with updates done as needed. The IT strategy and organization-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for determining the usage of internal and external resources required in system development and operations.

5 Optimized when

IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organization.

PO2 Define the Information Architecture

PO2 Maturity Model

Control over the IT process “Define the Information Architecture” with the business goal of being agile in responding to requirements, to provide reliable and consistent information, and to seamlessly integrate applications into business processes.

Measurement

0 Non-existent when

There is no awareness of the importance of the information architecture for the organization. The knowledge, expertise and responsibilities necessary to develop this architecture do not exist in the organization.

1 Initial/Ad Hoc when

Management recognizes the need for an information architecture. Development of some components of an information architecture is occurring on an ad hoc basis. The definitions address data, rather than information, and are driven by application software vendor offerings. There is inconsistent and sporadic communication of the need for an information architecture.

2 Repeatable but Intuitive when

An information architecture process emerges and similar, though informal and intuitive, procedures are followed by different individuals within the organization. Staff obtain their skills in building the information architecture through hands-on experience and repeated application of techniques. Tactical requirements drive the development of information architecture components by individual staff members.

3 Defined when

The importance of the information architecture is understood and accepted, and responsibility for its delivery is assigned and clearly communicated. Related procedures, tools and techniques, although not sophisticated, have been standardized and documented and are part of informal training activities. Basic information architecture policies have been developed, including some strategic requirements, but compliance with policies, standards and tools is not consistently enforced. A formally defined data administration function is in place, setting organization-wide standards, and is beginning to report on the delivery and use of the information architecture. Automated tools are beginning to be employed, but the processes and rules used are defined by database software vendor offerings. A formal training plan has been developed, but formalized training is still based on individual initiatives.

4 Managed and Measurable when

The development and enforcement of the information architecture are fully supported by formal methods and techniques. Accountability for the performance of the architecture development process is enforced and success of the information architecture is being measured. Supporting automated tools are widespread, but are not yet integrated. Basic metrics have been identified and a measurement system is in place. The information architecture definition process is proactive and focused on addressing future business needs. The data administration organization is actively involved in all application development efforts, to ensure consistency. An automated repository is fully implemented. More complex data models are being implemented to leverage the information content of the databases. Executive information systems and decision support systems are leveraging the available information.

5 Optimized when

The information architecture is consistently enforced at all levels. The value of the information architecture to the business is continually stressed. IT personnel have the expertise and skills necessary to develop and maintain a robust and responsive information architecture that reflects all the business requirements. The information provided by the information architecture is consistently and extensively applied. Extensive use is made of industry good practices in the development and maintenance of the information architecture, including a continuous improvement process. The strategy for leveraging information through data warehousing and data mining technologies is defined. The information architecture is continuously improving and takes into consideration non-traditional information on processes, organizations and systems.

PO4 Define the IT Processes, Organization and Relationships

PO4 Maturity Model

Control over the IT process “*Define the IT Processes, Organization and Relationships*” with the business goal of being agile in responding to the business strategy whilst complying with governance requirements and providing defined and competent points of contact.

Measurement

0 Non-existent when

The IT organization is not effectively established to focus on the achievement of business objectives.

1 Initial/Ad Hoc when

IT activities and functions are reactive and inconsistently implemented. IT is involved in business projects only in later stages. The IT function is considered a support function, without an overall organization perspective. There is an implicit understanding of the need for an IT organization; however, roles and responsibilities are neither formalized nor enforced.

2 Repeatable but Intuitive when

The IT function is organized to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured organization and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organization and vendor relationships.

3 Defined when

Defined roles and responsibilities for the IT organization and third parties exist. The IT organization is developed, documented, communicated and aligned with the IT strategy. The internal control environment is defined. There is formalization of relationships with other parties, including steering committees, internal audit and vendor management. The IT organization is functionally complete. There are definitions of the functions to be performed by IT personnel and those to be performed by users. Essential IT staffing requirements and expertise are defined and satisfied. There is a formal definition of relationships with users and third parties. The division of roles and responsibilities is defined and implemented.

4 Managed and Measurable when

The IT organization proactively responds to change and includes all roles necessary to meet business requirements. IT management, process ownership, accountability and responsibility are defined and balanced. Internal good practices have been applied in the organization of the IT functions. IT management has the appropriate expertise and skills to define, implement and monitor the preferred organization and relationships. Measurable metrics to support business objectives and user-defined critical success factors (CSFs) are standardized. Skill inventories are available to support project staffing and professional development. The balance between the skills and resources available internally and those needed from external organizations is defined and enforced. The IT organizational structure appropriately reflects the business needs by providing services aligned with strategic business processes, rather than with isolated technologies.

5 Optimized when

The IT organizational structure is flexible and adaptive. Industry good practices are deployed. There is extensive use of technology to assist in monitoring the performance of the IT organization and processes. Technology is leveraged in line to support the

complexity and geographic distribution of the organization. There is a continuous improvement process in place.

PO5 Managing the IT Investment

PO5 Maturity Model

Control over the IT process “Manage the IT Investment” with the business goal of continuously and demonstrably improving IT’s cost-efficiency and its contribution to business profitability with integrated and standardized services that satisfy end-user expectations.

Measurement

0 Non-existent when

There is no awareness of the importance of IT investment selection and budgeting. There is no tracking or monitoring of IT investments and expenditures.

1 Initial/Ad Hoc when

The organization recognizes the need for managing the IT investment, but this need is communicated inconsistently. Allocation of responsibility for IT investment selection and budget development is done on an ad hoc basis. Isolated implementations of IT investment selection and budgeting occur, with informal documentation. IT investments are justified on an ad hoc basis. Reactive and operationally focused budgeting decisions occur.

2 Repeatable but Intuitive when

There is an implicit understanding of the need for IT investment selection and budgeting. The need for a selection and budgeting process is communicated. Compliance is dependent on the initiative of individuals in the organization. There is an emergence of common techniques to develop components of the IT budget. Reactive and tactical budgeting decisions occur.

3 Defined when

Policies and processes for investment and budgeting are defined, documented and communicated, and cover key business and technology issues. The IT budget is aligned with the strategic IT and business plans. The budgeting and IT investment selection processes are formalized, documented and communicated. Formal training is emerging but is still based primarily on individual initiatives. Formal approval of IT investment selections and budgets is taking place. IT staff members have the expertise and skills necessary to develop the IT budget and recommend appropriate IT investments.

4 Managed and Measurable when

Responsibility and accountability for investment selection and budgeting are assigned to a specific individual. Budget variances are identified and resolved. Formal costing analysis is performed, covering direct and indirect costs of existing operations, as well as proposed investments, considering all costs over a total life cycle. A proactive and standardized process for budgeting is used. The impact of shifting in development and operating costs from hardware and software to systems integration and IT human

resources is recognized in the investment plans. Benefits and returns are calculated in financial and non-financial terms.

5 Optimized when

Industry good practices are used to benchmark costs and identify approaches to increase the effectiveness of investments. Analysis of technological developments is used in the investment selection and budgeting process. The investment management process is continuously improved based on lessons learned from the analysis of actual investment performance. Investment decisions incorporate price/performance improvement trends. Funding alternatives are formally investigated and evaluated within the context of the organization's existing capital structure, using formal evaluation methods. There is proactive identification of variances. An analysis of the long-term cost and benefits of the total life cycle is incorporated in the investment decisions.

PO8 Manage Quality

PO8 Maturity Model

Control over the IT process "Manage Quality" with the business goal of ensuring continuous and measurable improvement of the quality of IT services delivered.

Measurement

0 Non-existent when

The organization lacks a QMS planning process and a system development life cycle (SDLC) methodology. Senior management and IT staff members do not recognize that a quality program is necessary. Projects and operations are never reviewed for quality.

1 Initial/Ad Hoc when

There is a management awareness of the need for a QMS. The QMS is driven by individuals where it takes place. Management makes informal judgments on quality.

2 Repeatable but Intuitive when

A program is being established to define and monitor QMS activities within IT. QMS activities that do occur are focused on IT project- and process-oriented initiatives, not on organization-wide processes.

3 Defined when

A defined QMS process is communicated throughout the enterprise by management and involves IT and end-user management. An education and training program is emerging to teach all levels of the organization about quality. Basic quality expectations are defined and are shared amongst projects and within the IT organization. Common tools and practices for quality management are emerging. Quality satisfaction surveys are planned and occasionally conducted.

4 Managed and Measurable when

The QMS is addressed in all processes, including processes with reliance on third parties. A standardized knowledge base is being established for quality metrics. Cost-benefit analysis methods are used to justify QMS initiatives. Benchmarking against the

industry and competitors is emerging. An education and training program is instituted to teach all levels of the organization about quality. Tools and practices are being standardized, and root cause analysis is periodically applied. Quality satisfaction surveys are consistently conducted. A standardized program for measuring quality is in place and well structured. IT management is building a knowledge base for quality metrics.

5 Optimized when

The QMS is integrated and enforced in all IT activities. QMS processes are flexible and adaptable to changes in the IT environment. The knowledge base for quality metrics is enhanced with external good practices. Benchmarking against external standards is routinely performed. Quality satisfaction surveying is an ongoing process and leads to root cause analysis and improvement actions. There is formal assurance on the level of the quality management process.

PO10 Manage Projects

PO10 Maturity Model

Control over the IT process “Manage Projects” with the business goal of ensuring the delivery of project results within agreed-upon time frames, budget and quality.

Measurement

0 Non-existent when

Project management techniques are not used and the organization does not consider business impacts associated with project mismanagement and development project failures.

1 Initial/Ad Hoc when

The use of project management techniques and approaches within IT is a decision left to individual IT managers. There is a lack of management commitment to project ownership and project management. Critical decisions on project management are made without user management or customer input. There is little or no customer and user involvement in defining IT projects. There is no clear organization within IT for the management of projects. Roles and responsibilities for the management of projects are not defined. Projects, schedules and milestones are poorly defined, if at all. Project staff time and expenses are not tracked and compared to budgets.

2 Repeatable but Intuitive when

Senior management gains and communicates an awareness of the need for IT project management. The organization is in the process of developing and utilizing some techniques and methods from project to project. IT projects have informally defined business and technical objectives. There is limited stakeholder involvement in IT project management. Initial guidelines are developed for many aspects of project management. Application of project management guidelines is left to the discretion of the individual project manager.

3 Defined when

The IT project management process and methodology are established and

communicated. IT projects are defined with appropriate business and technical objectives. Senior IT and business management are beginning to be committed and involved in the management of IT projects. A project management office is established within IT, with initial roles and responsibilities defined. IT projects are monitored, with defined and updated milestones, schedules, budget and performance measurements. Project management training is available and is primarily a result of individual staff initiatives. QA procedures and post-system implementation activities are defined, but are not broadly applied by IT managers. Projects are beginning to be managed as portfolios.

4 Managed and Measurable when

Management requires formal and standardized project metrics and lessons learned to be reviewed following project completion. Project management is measured and evaluated throughout the organization and not just within IT. Enhancements to the project management process are formalized and communicated with project team members trained on enhancements. IT management implements a project organization structure with documented roles, responsibilities and staff performance criteria. Criteria for evaluating success at each milestone are established. Value and risk are measured and managed prior to, during and after the completion of projects. Projects increasingly address organization goals, rather than only IT-specific ones. There is strong and active project support from senior management sponsors as well as stakeholders. Relevant project management training is planned for staff in the project management office and across the IT function.

5 Optimized when

A proven, full life cycle project and program methodology is implemented, enforced and integrated into the culture of the entire organization. An ongoing initiative to identify and institutionalize best project management practices is implemented. An IT strategy for sourcing development and operational projects is defined and implemented. An integrated project management office is responsible for projects and programs from inception to post-implementation. Organization-wide planning of programs and projects ensures that user and IT resources are best utilized to support strategic initiatives.

AI2 Acquire and Maintain Application Software

AI2 Maturity Model

Control over the IT process “Acquire and Maintain Application Software” with the business goal of aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost.

Measurement

0 Non-existent when

There is no process for designing and specifying applications. Typically, applications are obtained based on vendor-driven offerings, brand recognition or IT staff familiarity with specific products, with little or no consideration of actual requirements.

1 Initial/Ad Hoc when

There is an awareness that a process for acquiring and maintaining applications is required. Approaches to acquiring and maintaining application software vary from project to project. Some individual solutions to particular business requirements are likely to have been acquired independently, resulting in inefficiencies with maintenance and support.

2 Repeatable but Intuitive when

There are different, but similar, processes for acquiring and maintaining applications based on the expertise within the IT function. The success rate with applications depends greatly on the in-house skills and experience levels within IT. Maintenance is usually problematic and suffers when internal knowledge is lost from the organization. There is little consideration of application security and availability in the design or acquisition of application software.

3 Defined when

A clear, defined and generally understood process exists for the acquisition and maintenance of application software. This process is aligned with IT and business strategy. An attempt is made to apply the documented processes consistently across different applications and projects. The methodologies are generally inflexible and difficult to apply in all cases, so steps are likely to be bypassed. Maintenance activities are planned, scheduled and coordinated.

4 Managed and Measurable when

There is a formal and well-understood methodology that includes a design and specification process, criteria for acquisition, a process for testing and requirements for documentation. Documented and agreed-upon approval mechanisms exist to ensure that all steps are followed and exceptions are authorized. Practices and procedures evolve and are well suited to the organization, used by all staff and applicable to most application requirements.

5 Optimized when

Application software acquisition and maintenance practices are aligned with the defined

process. The approach is component based, with predefined, standardized applications matched to business needs. The approach is enterprise wide. The acquisition and maintenance methodology is well advanced and enables rapid deployment, allowing for high responsiveness and flexibility in responding to changing business requirements. The application software acquisition and implementation methodology is subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and good practices. The methodology creates documentation in a predefined structure that makes production and maintenance efficient.

AI3 Acquire and Maintain Technology Infrastructure

AI3 Maturity Model

Control over the IT process "*Acquire and Maintain Technology Infrastructure*" with the business goal of acquiring and maintaining an integrated and standardized IT infrastructure.

Measurement

0 Non-existent when

Managing the technology infrastructure is not recognized as a sufficiently important topic to be addressed.

1 Initial/Ad Hoc when

There are changes made to infrastructure for every new application, without any overall plan. Although there is an awareness that the IT infrastructure is important, there is no consistent overall approach. Maintenance activity reacts to short-term needs. The production environment is the test environment.

2 Repeatable but Intuitive when

There is a consistency amongst tactical approaches when acquiring and maintaining the IT infrastructure. Acquisition and maintenance of IT infrastructure are not based on any defined strategy and do not consider the needs of the business applications that must be supported. There is an understanding that the IT infrastructure is important, supported by some formal practices. Some maintenance is scheduled, but it is not fully scheduled and coordinated. For some environments, a separate test environment exists.

3 Defined when

A clear, defined and generally understood process exists for acquiring and maintaining IT infrastructure. The process supports the needs of critical business applications and is aligned to IT and business strategy, but it is not consistently applied. Maintenance is planned, scheduled and coordinated. There are separate environments for test and production.

4 Managed and Measurable when

The acquisition and maintenance process for technology infrastructure has developed to the point where it works well for most situations, is followed consistently and is focused on reusability. The IT infrastructure adequately supports the business applications. The

process is well organized and proactive. The cost and lead time to achieve the expected level of scalability, flexibility and integration are partially optimized.

5 Optimized when

The acquisition and maintenance process for technology infrastructure is proactive and closely aligned with critical business applications and the technology architecture. Good practices regarding technology solutions are followed, and the organization is aware of the latest platform developments and management tools. Costs are reduced by rationalizing and standardizing infrastructure components and by using automation. A high level of technical awareness can identify optimum ways to proactively improve performance, including consideration of outsourcing options. The IT infrastructure is seen as the key enabler to leveraging the use of IT.

AI5 Procure IT Resources

AI5 Maturity Model

Control over the IT process “Procure IT Resources” with the business goal of improving IT’s cost-efficiency and its contribution to business profitability.

Measurement

0 Non-existent when

There is no defined IT resource procurement process in place. The organization does not recognize the need for clear procurement policies and procedures to ensure that all IT resources are available in a timely and cost-efficient manner.

1 Initial/Ad Hoc when

The organization recognizes the need to have documented policies and procedures that link IT acquisition to the business organization’s overall procurement process. Contracts for the acquisition of IT resources are developed and managed by project managers and other individuals exercising their professional judgment rather than as a result of formal procedures and policies. There is only an *ad hoc* relationship between corporate acquisition and contract management processes and IT. Contracts for acquisition are managed at the conclusion of projects rather than on a continuous basis.

2 Repeatable but Intuitive when

There is organizational awareness of the need to have basic policies and procedures for IT acquisition. Policies and procedures are partially integrated with the business organization’s overall procurement process. Procurement processes are mostly utilized for large and highly visible projects. Responsibilities and accountabilities for IT procurement and contract management are determined by the individual contract manager’s experience. The importance of supplier management and relationship management is recognized; however, it is addressed based on individual initiative. Contract processes are mostly utilized by large or highly visible projects.

3 Defined when

Management institutes policies and procedures for IT acquisition. Policies and procedures are guided by the business organization’s overall procurement process. IT

acquisition is largely integrated with overall business procurement systems. IT standards for the acquisition of IT resources exist. Suppliers of IT resources are integrated into the organization's project management mechanisms from a contract management perspective. IT management communicates the need for appropriate acquisitions and contract management throughout the IT function.

4 Managed and Measurable when

IT acquisition is fully integrated with overall business procurement systems. IT standards for the acquisition of IT resources are used for all procurements. Measurements on contract and procurement management are taken relevant to the business cases for IT acquisition. Reporting on IT acquisition activity that supports business objectives is available. Management is usually aware of exceptions to the policies and procedures for IT acquisition. Strategic management of relationships is developing. IT management enforces the use of the acquisition and contract management process for all acquisitions by reviewing performance measurement.

5 Optimized when

Management institutes resources' procurement thorough processes for IT acquisition. Management enforces compliance with policies and procedures for IT acquisition. Measurements on contract and procurement management are taken that are relevant to the business cases for IT acquisitions. Good relationships are established over time with most suppliers and partners, and the quality of relationships is measured and monitored. Relationships are managed strategically. IT standards, policies and procedures for the acquisition of IT resources are managed strategically and respond to measurement of the process. IT management communicates the strategic importance of appropriate acquisition and contract management throughout the IT function.

AI7 Install and Accredit Solutions and Changes

AI7 Maturity Model

Control over the IT process "Install and Accredit Solutions and changes" with the business goal of implementing new or changed systems that work without major problems after installation.

Measurement

0 Non-existent when

There is a complete lack of formal installation or accreditation processes, and neither senior management nor IT staff members recognize the need to verify that solutions are fit for the intended purpose.

1 Initial/Ad Hoc when

There is an awareness of the need to verify and confirm that implemented solutions serve the intended purpose. Testing is performed for some projects, but the initiative for testing is left to the individual project teams, and the approaches taken vary. Formal accreditation and sign-off are rare or non-existent.

2 Repeatable but Intuitive when

There is some consistency amongst the testing and accreditation approaches, but typically they are not based on any methodology. The individual development teams normally decide the testing approach, and there is usually an absence of integration testing. There is an informal approval process.

3 Defined when

A formal methodology relating to installation, migration, conversion and acceptance is in place. IT installation and accreditation processes are integrated into the system life cycle and automated to some extent. Training, testing and transition to production status and accreditation are likely to vary from the defined process, based on individual decisions. The quality of systems entering production is inconsistent, with new systems often generating a significant level of post-implementation problems.

4 Managed and Measurable when

The procedures are formalized and developed to be well organized and practical with defined test environments and accreditation procedures. In practice, all major changes to systems follow this formalized approach. Evaluation of meeting user requirements is standardized and measurable, producing metrics that can be effectively reviewed and analyzed by management. The quality of systems entering production is satisfactory to management even with reasonable levels of post-implementation problems. Automation of the process is *ad hoc* and project-dependent. Management may be satisfied with the current level of efficiency despite the lack of post-implementation evaluation. The test system adequately reflects the live environment. Stress testing for new systems and regression testing for existing systems are applied for major projects.

5 Optimized when

The installation and accreditation processes have been refined to a level of good practice, based on the results of continuous improvement and refinement. IT installation and accreditation processes are fully integrated into the system life cycle and automated when appropriate, facilitating the most efficient training, testing and transition to production status of new systems. Well-developed test environments, problem registers and fault resolution processes ensure efficient and effective transition to the production environment. Accreditation usually takes place with no rework, and post-implementation problems are normally limited to minor corrections. Post-implementation reviews are standardized, with lessons learned channeled back into the process to ensure continuous quality improvement. Stress testing for new systems and regression testing for modified systems are consistently applied.

DS1 Define and Manage Service Levels

DS1 Maturity Model

Control over the IT process “Define and Manage Service Levels” with the business goal of ensuring the alignment of key IT services with the business strategy.

Measurement

0 Non-existent when

Management has not recognized the need for a process for defining service levels. Accountabilities and responsibilities for monitoring them are not assigned.

1 Initial/Ad Hoc when

There is awareness of the need to manage service levels, but the process is informal and reactive. The responsibility and accountability for defining and managing services are not defined. If performance measurements exist, they are qualitative only with imprecisely defined goals. Reporting is informal, infrequent and inconsistent.

2 Repeatable but Intuitive when

There are agreed-upon service levels, but they are informal and not reviewed. Service level reporting is incomplete and may be irrelevant or misleading for customers. Service level reporting is dependent on the skills and initiative of individual managers. A service level co-coordinator is appointed with defined responsibilities, but limited authority. If a process for compliance to SLAs exists, it is voluntary and not enforced.

3 Defined when

Responsibilities are well defined, but with discretionary authority. The SLA development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to, but they may not address business needs.

4 Managed and Measurable when

Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardized and reflect industry norms. The criteria for defining service levels are based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood. A formal system of measurement is instituted and maintained.

5 Optimized when

Service levels are continuously re-evaluated to ensure alignment of IT and business objectives, whilst taking advantage of technology, including the cost-benefit ratio. All service level management processes are subject to continuous improvement. Customer satisfaction levels are continuously monitored and managed. Expected service levels reflect strategic goals of business units and are evaluated against industry norms. IT management has the resources and accountability needed to meet service level targets, and compensation is structured to provide incentives for meeting these targets. Senior management monitors performance metrics as part of a continuous improvement process.

DS2 Manage Third-party Services

DS2 Maturity Model

Control over the IT process “Manage Third-party Services” with the business goal of providing satisfactory third-party services whilst being transparent about benefits, costs and risks.

Measurement

0 Non-existent when

Responsibilities and accountabilities are not defined. There are no formal policies and procedures regarding contracting with third parties. Third-party services are neither approved nor reviewed by management. There are no measurement activities and no reporting by third parties. In the absence of a contractual obligation for reporting, senior management is not aware of the quality of the service delivered.

1 Initial/Ad Hoc when

Management is aware of the need to have documented policies and procedures for third-party management, including signed contracts. There are no standard terms of agreement with service providers. Measurement of the services provided is informal and reactive. Practices are dependent on the experience (e.g., on demand) of the individual and the supplier.

2 Repeatable but Intuitive when

The process for overseeing third-party service providers, associated risks and the delivery of services is informal. A signed, *pro forma* contract is used with standard vendor terms and conditions (e.g., the description of services to be provided). Reports on the services provided are available, but do not support business objectives.

3 Defined when

Well-documented procedures are in place to govern third-party services, with clear processes for vetting and negotiating with vendors. When an agreement for the provision of services is made, the relationship with the third party is purely a contractual one. The nature of the services to be provided is detailed in the contract and includes legal, operational and control requirements. The responsibility for oversight of third-party services is assigned. Contractual terms are based on standardized templates. The business risk associated with the third-party services is assessed and reported.

4 Managed and Measurable when

Formal and standardized criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned. Vendor qualifications, risks and capabilities are verified on a continual basis. Service requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to assess current and future third-party services. Transfer pricing models are used in the procurement process. All parties involved are aware of service, cost and milestone expectations. Agreed-upon goals and metrics for the oversight of service providers exist.

5 Optimized when

Contracts signed with third parties are reviewed periodically at predefined intervals. The responsibility for managing suppliers and the quality of the services provided is assigned. Evidence of contract compliance to operational, legal and control provisions is monitored, and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery. Measurements vary in response to changing business conditions. Measures support early detection of potential problems with third-party services. Comprehensive, defined reporting of service level achievement is linked to the third-party compensation. Management adjusts the process of third-party service acquisition and monitoring based on the measurers.

DS10 Manage Problems

DS10 Maturity Model

Control over the IT process “Manage Problems” with the business goal of ensuring end users’ satisfaction with service offerings and service levels, and reducing solution and service delivery defects and rework.

Measurement

0 Non-existent when

There is no awareness of the need for managing problems, as there is no differentiation of problems and incidents. Therefore, there is no attempt made to identify the root cause of incidents.

1 Initial/Ad Hoc when

Personnel recognize the need to manage problems and resolve underlying causes. Key knowledgeable personnel provide some assistance with problems relating to their area of expertise, but the responsibility for problem management is not assigned. Information is not shared, resulting in additional problem creation and loss of productive time while searching for answers.

2 Repeatable but Intuitive when

There is a wide awareness of the need for and benefits of managing IT-related problems

within both the business units and information services function. The resolution process is evolved to a point where a few key individuals are responsible for identifying and resolving problems. Information is shared amongst staff in an informal and reactive way. The service level to the user community varies and is hampered by insufficient, structured knowledge available to the problem manager.

3 Defined when

The need for an effective integrated problem management system is accepted and evidenced by management support, and budgets for the staffing and training are available. Problem resolution and escalation processes have been standardized. The recording and tracking of problems and their resolutions are fragmented within the response team, using the available tools without centralization. Deviations from established norms or standards are likely to be undetected. Information is shared among staff in a proactive and formal manner. Management review of incidents and analysis of problem identification and resolution are limited and informal.

4 Managed and Measurable when

The problem management process is understood at all levels within the organization. Responsibilities and ownership are clear and established. Methods and procedures are documented, communicated and measured for effectiveness. The majority of problems are identified, recorded and reported, and resolution is initiated. Knowledge and expertise are cultivated, maintained and developed to higher levels, as the function is viewed as an asset and major contributor to the achievement of IT objectives and improvement of IT services. Problem management is well integrated with interrelated processes, such as incident, change, availability and configuration management, and assists customers in managing data, facilities and operations. Goals and metrics have been agreed upon for the problem management process.

5 Optimized when

The problem management process is evolved into a forward-looking and proactive one, contributing to the IT objectives. Problems are anticipated and prevented. Knowledge regarding patterns of past and future problems is maintained through regular contacts with vendors and experts. The recording, reporting and analysis of problems and resolutions are automated and fully integrated with configuration data management. Goals are measured consistently. Most systems have been equipped with automatic detection and warning mechanisms, which are continuously tracked and evaluated. The problem management process is analyzed for continuous improvement based on analysis of measures and is reported to stakeholders.

ME1 Monitor and Evaluate IT Performance

ME1 Maturity Model

Control over the IT process “Monitor and Evaluate IT Performance” with the business goal of transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements.

Measurement

0 Non-existent when

The organization has no monitoring process implemented. IT does not independently perform monitoring of projects or processes. Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognized.

1 Initial/Ad Hoc when

Management recognizes a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organization. The accounting function monitors basic financial measures for IT.

2 Repeatable but Intuitive when

Basic measurements to be monitored are identified. Collection and assessment methods and techniques exist, but the processes are not adopted across the entire organization. Interpretation of monitoring results is based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but the gathering is not based on a planned approach.

3 Defined when

Management communicates and institutes standard monitoring processes. Educational and training programs for monitoring are implemented. A formalized knowledge base of historical performance information is developed. Assessment is still performed at the individual IT process and project level and is not integrated amongst all processes. Tools for monitoring IT processes and service levels are defined. Measurements of the contribution of the information services function to the performance of the organization are defined, using traditional financial and operational criteria. IT-specific performance measurements, non-financial measurements, strategic measurements, customer satisfaction measurements and service levels are defined. A framework is defined for measuring performance.

4 Managed and Measurable when

Management defines the tolerances under which processes must operate. Reporting of monitoring results is being standardized and normalized. There is integration of metrics across all IT projects and processes. The IT organization’s management reporting systems are formalized. Automated tools are integrated and leveraged organization-wide to collect and monitor operational information on applications, systems and processes. Management is able to evaluate performance based on agreed-upon criteria approved

by stakeholders. Measurements of the IT function align with organization-wide goals.

5 Optimized when

A continuous quality improvement process is developed for updating organization-wide monitoring standards and policies and incorporating industry good practices. All monitoring processes are optimized and support organization-wide objectives. Business driven metrics are routinely used to measure performance and are integrated into strategic assessment frameworks, such as the IT balanced scorecard. Process monitoring and ongoing redesign are consistent with organization-wide business process improvement plans. Benchmarking against industry and key competitors becomes formalized, with well-understood comparison criteria.

ME3 Ensure Compliance with External Requirements

ME3 Maturity Model

Control over the IT process “Ensure Compliance with External Requirements” with the business goal of ensuring compliance with laws, regulations and contractual requirements.

Measurement

0 Non-existent when

There is little awareness of external requirements that affect IT, with no process regarding compliance with regulatory, legal and contractual requirements.

1 Initial/Ad Hoc when

There is awareness of regulatory, contractual and legal compliance requirements impacting the organization. Informal processes are followed to maintain compliance, but only as the need arises in new projects or in response to audits or reviews.

2 Repeatable but Intuitive when

There is an understanding of the need to comply with external requirements, and the need is communicated. Where compliance is a recurring requirement, as in financial regulations or privacy legislation, individual compliance procedures have been developed and are followed on a year-to-year basis. There is, however, no standard approach. There is high reliance on the knowledge and responsibility of individuals, and errors are likely. There is informal training regarding external requirements and compliance issues.

3 Defined when

Policies, plans and procedures are developed, documented and communicated to ensure compliance with regulations and contractual and legal obligations, but some may not always be followed, and some may be out of date or impractical to implement. There is little monitoring performed and there are compliance requirements that have not been addressed. Training is provided in external legal and regulatory requirements affecting the organization and the defined compliance processes. Standard *pro forma* contracts and legal processes exist to minimize the risks associated with contractual liability.

4 Managed and Measurable when

Issues and exposures from external requirements and the need to ensure compliance at all levels are fully understood. A formal training scheme is in place to ensure that all staff members are aware of their compliance obligations. Responsibilities are clear and process ownership is understood. The process includes a review of the environment to identify external requirements and ongoing changes. There is a mechanism in place to monitor non-compliance with external requirements, enforce internal practices and implement corrective action. Non-compliance issues are analyzed for root causes in a standard manner, with the objective to identify sustainable solutions. Standardized internal good practices are utilized for specific needs, such as standing regulations and recurring service contracts.

5 Optimized when

A well-organized, efficient and enforced process is in place for complying with external requirements, based on a single central function that provides guidance and co-ordination to the whole organization. Extensive knowledge of the applicable external requirements, including their future trends and anticipated changes, and the need for new solutions exist. The organization takes part in external discussions with regulatory and industry groups to understand and influence external requirements affecting them. Good practices are developed ensuring efficient compliance with external requirements, resulting in very few cases of compliance exceptions. A central, organization-wide tracking system exists, enabling management to document the workflow and to measure and improve the quality and effectiveness of the compliance monitoring process. An external requirements self-assessment process is implemented and refined to a level of good practice. The organization's management style and culture relating to compliance are sufficiently strong, and processes are developed well enough for training to be limited to new personnel and whenever there is a significant change.

ME4 Provide IT Governance

ME4 Maturity Model

Control over the IT process "Provide IT Governance" with the business goal of integrating IT governance with corporate governance objectives and complying with laws and regulations.

Measurement

0 Non-existent when

There is a complete lack of any recognizable IT governance process. The organization does not even recognize that there is an issue to be addressed; hence, there is no communication about the issue.

1 Initial/Ad Hoc when

There is recognition that IT governance issues exist and need to be addressed. There are *ad hoc* approaches applied on an individual or case-by-case basis. Management's approach is reactive, and there is only sporadic, inconsistent communication on issues and approaches to address them. Management has only an approximate indication of how IT contributes to business performance. Management only reactively responds to

an incident that has caused some loss or embarrassment to the organization.

2 Repeatable but Intuitive when

There is awareness of IT governance issues. IT governance activities and performance indicators, which include IT planning, delivery and monitoring processes, are under development. Selected IT processes are identified for improvement based on individuals' decisions. Management identifies basic IT governance measurements and assessment methods and techniques; however, the process is not adopted across the organization. Communication on governance standards and responsibilities is left to the individual. Individuals drive the governance processes within various IT projects and processes. The processes, tools and metrics to measure IT governance are limited and may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined when

The importance of and need for IT governance are understood by management and communicated to the organization. A baseline set of IT governance indicators is developed where linkages between outcome measures and performance indicators are defined and documented. Procedures are standardized and documented. Management communicates standardized procedures, and training is established. Tools are identified to assist with overseeing IT governance. Dashboards are defined as part of the IT balanced business scorecard. However, it is left to the individual to get training, follow the standards and apply them. Processes may be monitored, but deviations, while mostly being acted upon by individual initiative, are unlikely to be detected by management.

4 Managed and Measurable when

There is full understanding of IT governance issues at all levels. There is a clear understanding of who the customer is, and responsibilities are defined and monitored through SLAs. Responsibilities are clear and process ownership is established. IT processes and IT governance are aligned with and integrated into the business and the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding, and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management defines tolerances under which processes must operate. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. IT governance has been integrated into strategic and operational planning and monitoring processes. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise wide improvements. Overall accountability of key process performance is clear, and management is rewarded based on key performance measures.

5 Optimized when

There is an advanced and forward-looking understanding of IT governance issues and solutions. Training and communication are supported by leading-edge concepts and techniques. Processes are refined to a level of industry good practice, based on results of continuous improvement and maturity modeling with other organizations. The implementation of IT policies leads to an organization, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analyzed, and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimized manner to automate the

workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organization, and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise. IT governance activities are integrated with the enterprise governance process.

MAPPING NIST 800-53 REV 3 WITH COBIT 4.1

Control Objective		NIST SP 800-53 Revision 3	
		Coverage	**Requirements**
Plan and Organize			
PO1	Define a Strategic IT Plan	A	SA-2, CA-7, and CM-2
PO2	Define the Information Architecture	A	CM-1, CM-2, AC-3, SI-1, SI-4, SI-7, SI-10
PO4	Define the IT Processes, Organization and Relationships	A	AC-5, AC-6, PS-2, PS-7
PO5	Manage the IT Investment	A	SA-2
PO8	Manage Quality	A	SA-3
PO10	Manage Projects	A	CA-1
Acquire and Implement			
AI2	Acquire and Maintain Application Software	A	AU-2, SI-7, SI-10, SA-1, SA-3, SA-4, SA-8, SA-11, AC-3, IA-2, MA-2, and SC-2
AI3	Acquire and Maintain Technology Infrastructure	A	SA-3, SA-4, SA-8, SA-11, MA-2
AI5	Procure IT Resources	A	SA-1 and SA-4
AI7	Install and Accredit Solutions and Changes	A	CA-4 and CA-6
Deliver and Support			
DS1	Define and Manage Service Levels	A	SA-9
DS2	Manage Third-party Services	A	PS-7 and SA-9
DS10	Manage Problems	N/A	
Monitor and Evaluate			
ME1	Monitor and Evaluate IT Performance	N/A	
ME3	Ensure Compliance with External Requirements	N/A	
ME4	Provide IT Governance	N/A	

Legend: (A) Some aspects are addressed
(N/A) Not addressed