Evaluation Report

OIG-CA-21-003

INFORMATION TECHNOLOGY: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2020

October 26, 2020

Office of
Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 26, 2020

MEMORANDUM FOR **BEN SCAGGS**
EXECUTIVE DIRECTOR

FROM: Larissa Klimpel /s/
Director, Cyber/Information Technology Audit

SUBJECT: Evaluation Report – *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation for Fiscal Year 2020* (OIG-CA-21-003)

We hereby transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2020*, dated October 26, 2020. The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security for the collection of annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with RMA Associates LLC (RMA), an independent certified public accounting firm, to perform this year's annual FISMA evaluation of the Gulf Coast Ecosystem Restoration Council's (Council) security program and practices for the period July 1, 2019 through June 30, 2020. RMA conducted its evaluation in accordance with *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*. In connection with our contract with RMA, we reviewed its report and related documentation and inquired of its representatives. Our review, as differentiated from an evaluation performed in accordance with inspection and evaluation standards, was not intended to enable us to conclude on the effectiveness of the Council's information security program and practices or its compliance with FISMA. RMA is responsible for its report and the conclusions expressed therein.

In brief, RMA reported that consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology standards and guidelines, the Council's information security program and practices

were established and have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains. RMA found that the Council's information security program and practices were effective for the period July 1, 2019 through June 30, 2020.

Appendix I of the attached RMA report includes the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*

If you have any questions or require further information, you may contact me at (202) 927-0361.

Attachment

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014

Evaluation Report for Fiscal Year 2020

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

October 26, 2020

Richard K. Delmar
Deputy Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Room 4436
Washington, DC 20220

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2020

Dear Mr. Delmar:

RMA Associates, LLC is pleased to submit the Gulf Coast Ecosystem Restoration Council (Council) Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2020. We conducted the evaluation in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*. We have also prepared the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014(FISMA) Reporting Metrics Version 4.0* (April 17, 2020) as shown in Appendix I. These metrics provide reporting requirements across the function areas to be addressed in the independent assessment of agencies' information security programs. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period July 1, 2019 through June 30, 2020.

In summary, we found that the Council's information security program and practices were effective for the period July 1, 2019 through June 30, 2020.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Table of Contents

Abbreviations ..... *ii*

Introduction *3*

Summary Evaluation Results *3*

Background *4*

Evaluation Results *7*

Objective, Scope, and Methodology *10*

Criteria *12*

Appendix I: FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics *14*

Key Changes to the FY 2020 IG FISMA Metrics 15

Identify Function Area 16

Protect Function Area 29

Detect Function Area 61

Respond Function Area 67

Recover Function Area 75

Appendix II: Management Response *83*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Abbreviations

ARC	Administrative Resource Center
BIA	Business Impact Analysis
CIO	Chief Information Officer
Council	Gulf Coast Ecosystem Restoration Council
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
GCC	Gulf Coast Council
ICAM	Identity Credential and Access Management
ICT	Information and Communications Technology
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSN	Office Support Network
PII	Personally Identifiable Information
PIPER	Program Information Platform for Ecosystem Restoration
POA&M	Plan of Action and Milestones
RAAMS	Restoration Assistance and Awards Management System
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SP	Special Publication
TIC	Trusted Internet Connection
Treasury	Department of the Treasury

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Introduction

This report presents the results of our independent evaluation of the Gulf Coast Ecosystem Restoration Council's (Council) information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA) requires Federal agencies to have an annual independent evaluation of their information security program and practices performed to determine the effectiveness of such program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. DHS prepared the FISMA questionnaire to collect the responses, which is provided in Appendix I: *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FISMA Reporting Metrics). We also considered applicable OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines.

FISMA requires the agency Inspector General (IG) or an independent external auditor, as determined by the IG, to perform the annual evaluation. The Department of the Treasury (Treasury) Office of Inspector General (OIG) engaged RMA Associates, LLC to conduct an annual evaluation of the Council's information security program and practices in support of the FISMA evaluation requirement. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period July 1, 2019, through June 30, 2020.

This evaluation was performed in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*. We have also prepared the FISMA Reporting Metrics, as shown in Appendix I. These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs. See *Objective, Scope, and Methodology* for more detail.

Summary Evaluation Results

We concluded, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and maintained for the five Cybersecurity Functions[1] and eight FISMA Metric Domains.[2] The overall maturity level of the Council's information security program was determined as Managed and Measurable, as described in this report. Accordingly, we found that the Council's information security program and practices were effective for the period July 1, 2019 through June 30, 2020.

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The eight FISMA Metric Domains were aligned with the five functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[2] As described in the FISMA Reporting Metrics, the eight FISMA Metric Domains are: (1) risk management, (2) configuration management, (3) identity and access management, (4) data protection and privacy, (5) security training, (6) information security continuous monitoring, (7) incident response, and (8) contingency planning.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

We provided the Council a draft of this report for comment. In a written response, management agreed with the results of our evaluation. See *Management's Response* in Appendix II for Council's response in its entirety.

Background

Gulf Coast Ecosystem Restoration Council

Spurred by the Deepwater Horizon oil spill, the *Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012* (RESTORE Act) was signed into law on July 6, 2012. The RESTORE Act calls for a regional approach to restoring the long-term health of the valuable natural ecosystem and economy of the Gulf Coast region. The RESTORE Act dedicates 80 percent of civil and administrative penalties paid under the Clean Water Act, after the date of enactment, by responsible parties in connection with the Deepwater Horizon oil spill to the Gulf Coast Restoration Trust Fund for ecosystem restoration, economic recovery, and tourism promotion in the Gulf Coast region.

In addition to creating the Gulf Coast Restoration Trust Fund, the RESTORE Act established the Council. The Council is comprised of a Chairperson from a member Federal agency and includes the Governors of the states of Alabama, Florida, Louisiana, Mississippi, and Texas, and the Secretaries or designees of the U.S. Departments of Agriculture, Army, Commerce, Homeland Security, and Interior, and the Administrator of the U.S. Environmental Protection Agency.

The Council is a small agency with a simple, flat organizational structure. The Council had few information technology (IT) assets and approximately 30 employees and contractors. The Council's information system infrastructure consists of an office network and several system service providers. The Council's Office Support Network (OSN) is technically not a computer network as it does not include any network servers. OSN is a stand-alone group of laptops connected to a leased wireless access point that provides a leased virtual private network connection to the Trusted Internet Connection (TIC) portal.

These system service providers host and support the Council's cloud-based systems and functions:

1. For payroll processing, the Council used WebTA hosted by the National Finance Center.
2. For financial management and report processing, the Council used the Treasury's Bureau of the Fiscal Service's Administrative Resource Center (ARC).
3. For grants processing, the Council used the Restoration Assistance and Awards Management System (RAAMS) hosted by the U.S. Geological Survey.[3]
4. For award management, the Council used GrantSolutions, a grant management service provider under the U.S. Department of Health and Human Services.

[3] RAAMS was replaced with GrantSolutions for award management and the Program Information Platform for Ecosystem Restoration (PIPER) for program data management. RAAMS was in the process of being decommissioned and running for internal use only at the time of this evaluation. The system turn off is scheduled for October 1, 2020.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

5. For program data, the Council used Program Information Platform for Ecosystem Restoration (PIPER), provided by U.S. Geological Survey hosting services. Website support was also provided by the U.S. Geological Survey hosting services.
6. For electronic records management, the Council used the National Archives and Records Administration.
7. For email and G Suite, the Council used the National Oceanic and Atmospheric Administration.
8. For Continuous Diagnostic Monitoring and Einstein Capabilities, the Council used the DHS.

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, required each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA amended the *Federal Information Security Management Act of 2002* and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthened use of continuous monitoring in systems, and increased focus on the agencies for compliance and reporting that is more concentrated on the issues caused by security incidents.

FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (known as the Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, "Managing Federal Information as a Strategic Resource," requires executive agencies within the Federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their systems; and
- Authorize system processing prior to operations and periodically after that.

These management responsibilities presume responsible agency officials understand the risks, and other factors, which could adversely affect their missions. Moreover, these officials must understand the current status of their security programs, and the security controls planned or in place, to protect their information and systems to make informed judgments and investments which appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST also developed an integrated Risk Management Framework which effectively brings together all the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

FISMA Reporting Metrics

We evaluated the effectiveness of the information security program and practices on a maturity model spectrum in which the foundation levels ensure the development of sound policies and procedures. The FISMA Reporting Metrics classify information security program and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security:

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures were lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Our evaluation was conducted for the period between July 1, 2019 and June 30, 2020. It consisted of testing the 67 metric questions listed in the FISMA Reporting Metrics issued by DHS. The answers to the 67 metric questions in Appendix I reflect the results of our testing of the Council's information security program and practices. The FISMA Reporting Metrics were aligned with the five Cybersecurity Framework security functions areas (key performance areas) as follows:

- Identify, which includes questions pertaining to Risk Management;
- Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- Detect, which includes questions pertaining to Information Security Continuous Monitoring;
- Respond, which includes questions pertaining to Incident Response; and
- Recover, which includes questions pertaining to Contingency Planning.

Evaluation Results

We determined the maturity level for each FISMA domain based on the responses to the questions contained in the FISMA Reporting Metrics and testing for each domain. For each domain, our determination considered the fact the Council is a small organization, which allows it to operate more efficiently and effectively compared to larger Federal agencies. The Council replaced the RAAMS system, which was being decommissioned at the time of this evaluation, with GrantSolutions for award management and PIPER for program data management. Since these systems were also cloud-based, the Council's IT controls, processes, and personnel did not change since the prior year's FISMA evaluation. We considered the Chief Information Officer (CIO) was closely involved in all aspects of the Council's IT environment and was aware of every important decision regarding the Council's IT operations. The overall maturity level of the Council's information security program was determined as Managed and Measurable based upon a simple majority of the component scores for each domain's maturity level, and due to the CIO's direct involvement in every IT security decision, his direct oversight of security controls, and the simple IT structure of stand-alone laptops and service vendors. Our tests of effectiveness found no exceptions.

Below is the maturity level for each domain.

Risk Management: We determined the Council's overall maturity level for the Risk Management program was Managed and Measurable. The Council defined the priority levels for the OSN and considered risks from the supporting business functions and mission impacts to help its leadership make informed risk management decisions. Those informed risk management decisions helped to continually improve and update the Council's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Risk Management program controls in place were effective.

Configuration Management: We determined the Council's overall maturity level for the Configuration Management program was Managed and Measurable. Given the Council did not own a network server, and did not have a general support system, its primary configuration management considerations were related to the standard configuration of their laptops. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's Configuration Management program controls in place were effective.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management program was Consistently Implemented. The Council had to manage the Identity, Credential, and Access Management (ICAM) protocols for approximately 30 employees and contractors. Due to the Council's size and structure with all systems, except the OSN, being cloud-based and housed by third parties, the Council did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews which were necessary to reach the Managed and Measurable level. Although the maturity level of this domain was Consistently Implemented, our control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Identity and Access Management program controls in place were effective.

Data Protection and Privacy: We determined the Council's overall maturity level for the Data Protection and Privacy program was Consistently Implemented. The Council did not process Personally Identifiable Information (PII) data as PII needed for human resources and payroll were handled through agreements with ARC and WebTA whose systems were approved to collect and process PII. Controls over PII were the responsibility of the Council's outsourced service providers. Therefore, the Council did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and use the information to make needed adjustments that were necessary to reach the Managed and Measurable level. Although the maturity level of this domain was Consistently Implemented, our control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Data Protection and Privacy program controls in place were effective.

Security Training: We determined the Council's overall maturity level for the Security Training program was Managed and Measurable. The Council had approximately 30 employees and contractors. Our testing of employees' security awareness and role-based training found no exceptions, and the controls were operating as intended. We concluded the Council's Security Training program controls in place were effective.

Information Security and Continuous Monitoring: We determined the Council's overall maturity level for the Information Security Continuous Monitoring (ISCM) program was Managed and Measurable. Decisions regarding IT operations were made with the direct involvement and approval of the Council's CIO, allowing leadership to monitor and analyze the effectiveness of its ISCM program. Our testing found no exceptions, and the controls were operating as intended. We concluded the Council's ISCM program controls in place were effective.

Incident Response: We determined the Council's overall maturity level for the Incident Response program was Consistently Implemented. Given the Council did not own network servers and had no general support system, the Council had limited exposure to the possibility of security incidents. The Council only had part-time incident response team members who served more as a virtual incident response team. The small organizational structure enabled the Council to respond to and address security incidents quickly. As a result, the Council's Computer Security Incident Response Center could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. Although the maturity level of this domain was Consistently Implemented, our control

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

testing for this domain found no exceptions, and the controls were operating as intended. As the Council's systems, with the exception of OSN, were managed by third party providers, the controls necessary to reach Managed and Measurable such as profiling techniques were the responsibility of the third party providers. We concluded the Council's Incident Response program controls in place were effective.

Contingency Planning: We determined the Council's overall maturity level for the Contingency Planning program was Consistently Implemented. Given the Council did not own any network servers and did not have a general support system, it developed policies and procedures for Contingency Planning which were consistently implemented but did not develop quantitative and qualitative effectiveness measures necessary to reach the Managed and Measurable level. As the Council's systems, with the exception of OSN, were managed by third party providers, controls such as quantitative and qualitative measures to reach the Managed and Measurable maturity level were the responsibility of the third party providers. Although the maturity level of this domain was Consistently Implemented, our control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Contingency Planning program controls in place were effective.

We concluded, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and had been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains. We found the Council's information security program and practices were effective for the period July 1, 2019 through June 30, 2020, and the overall maturity level of the Council's information security program was Managed and Measurable.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Objective, Scope, and Methodology

Objective

The objective of this evaluation was to determine the effectiveness of the Gulf Coast Ecosystem Restoration Council's (Council) information security program and practices for the period of July 1, 2019 through June 30, 2020.

Scope

The scope of our work included the Council's Office Support Network (OSN) and the following cloud-based systems and services supported by third party providers: National Finance Center's WebTA, Bureau of the Fiscal Service's Administrative Resource Center, U.S. Geological Survey's Restoration Assistance and Awards Management System and Program Information Platform for Ecosystem Restoration, U.S. Department of Health and Human Services' GrantSolutions, National Archives and Records Administration's electronic records management, National Oceanic and Atmospheric Administration's email and G Suite, and Department of Homeland Security's Continuous Diagnostic Monitoring and Einstein capabilities. OSN is technically not a computer network as it does not include any network servers. OSN is a stand-alone group of laptops connected to a leased wireless access point that provides a leased virtual private network connection to the Trusted Internet Connection portal. Our evaluation was conducted for the period between July 1, 2019, and June 30, 2020.

We determined the effectiveness of the Council's security program and practices by evaluating the following five Cybersecurity Framework security functions (key performance areas) outlined in the annual *FY 2020 Inspector General Federal Information Security Modernization Act of 2014(FISMA) Reporting Metrics Version 4.0* (April 17, 2020) (FISMA Reporting Metrics) as follows:

- Identify, which includes questions pertaining to Risk Management;
- Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, which includes questions pertaining to Information Security Continuous Monitoring;
- Respond, which includes questions pertaining to Incident Response; and
- Recover, which includes questions pertaining to Contingency Planning.

Methodology

The overall strategy of our evaluation considered National Institute of Standards and Technology

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

(NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* the FISMA guidance from the Council of Inspectors General on Integrity and Efficiency, Office of Management and Budget (OMB), and Department of Homeland Security (DHS), and the Council's policies and procedures. Our report shows the FISMA questions followed by the narrative of the maturity level, the criteria, and our test procedures. Our testing procedures were developed from NIST SP 800-53A Revision 4. For each of the FISMA questions, we indicated whether each maturity level was achieved by the Council by stating "PASS" or "NOT MET." We determined the overall maturity level of each of the eight domains by a simple majority of the component scores of the maturity level of each question within the domain, in accordance with the FISMA Reporting Metrics.

We conducted interviews with Council officials and reviewed legal and regulatory requirements stipulated in FISMA. We also examined documents supporting the information security program and practices. Where appropriate, we compared documents, such as the Council's IT policies and procedures, to requirements stipulated in NIST special publications. Also, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In testing for the effectiveness of the security controls relevant to the 67 metric questions, we tested the entire population of administrative controls of the Council. The application controls were the responsibility of the Council's service providers.

We conducted the FISMA evaluation in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*, issued January 2012, and subsequent revisions, OMB guidance,[4] FISMA Reporting Metrics, NIST guidance,[5] and the Council's policies and procedures.

[4] OMB Circular No. A-130, "*Managing Information as a Strategic Resource"* and M-20-04*, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements,* dated November 19, 2019.
[5] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations dated April, 2013;* and NIST *Framework for Improving Critical Infrastructure Cybersecurity version 1.1, dated April 16, 2018.*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Criteria

We focused our FISMA evaluation approach on Federal information security guidelines developed by the Council, NIST, and OMB. NIST SPs provide guidelines that were considered essential to the development and implementation of the Council's security programs. The following is a listing of the criteria used in the performance of the Fiscal Year 2020 FISMA evaluation:

Council

- Gulf Coast Council (GCC)-IT-06-AC-Access Control Policy
- GCC-IT-07-AU-Audit and Accountability Procedures
- GCC-IT-08-AT-Awareness and Training Procedures
- GCC-IT-09-CM-Configuration Management Procedures
- GCC-IT-10-CP-Contingency Planning Procedures
- GCC-IT-11-IA-Identification and Authentication Procedure
- GCC-IT-12-IR-Incident Response Procedures
- GCC-IT-13-MA-System Maintenance Policy and Procedures
- GCC-IT-14-MP-Media protection Procedures
- GCC-IT-15-PP-Personnel Security
- GCC-IT-16-PE-Physical and Environmental Protection
- GCC-IT-17-Pl-Security Planning Policy and Procedures
- GCC-IT-19-RA-Risk Assessment Procedures
- GCC-IT-20-CC-Security Assessment and Authorization Procedures
- GCC-IT-21-SC Security Assessment and Authorization
- GCC-IT-22-SI System and Information Integrity Procedures
- GCC-IT-23-SA-System and Services Acquisitions
- GCC-IT-24-Mobile Device Policy
- GCC-IT-25-Mobile Code Technologies
- GCC-IT-26-Sanitization Procedures

NIST Federal Information Processing Standards (FIPS) and Special Publications

- FIPS Publication 199*, Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200*, Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Prevention and Handling*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems, and Organizations*
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-20-04 *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Appendix I: FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Key Changes to the FY 2020 IG FISMA Metrics

The *FY 2020 CIO FISMA Metrics* includes an additional focus on the security of mobile devices (Government-Furnished Equipment and non-Government-Furnished-Equipment), particularly in the areas of mobile device management and enterprise mobility management. As such, the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014(FISMA) Reporting Metrics Version 4.0* (April 17, 2020) (FISMA Reporting Metrics) include updates to questions on asset management, security architecture, and flaw remediation (Questions #2, #3, #6, and #19) to assess agency progress in securing mobile endpoints and employing secure application development processes.

Furthermore, the Office of Management and Budget (OMB) issued OMB Memorandum M-19-26, *Update to the Trusted Internet Connection (TIC) Initiative*, September 12, 2019, that provided updated guidance to federal agencies on the use of TIC capabilities in modern architectures and frameworks such as cloud environments. While the memorandum gives agencies until September 2020 to implement new TIC requirements, the FISMA Reporting Metric on TIC implementation (Question #20) has been updated to assess the agency's progress in planning for the effective implementation of the security capabilities outlined in OMB M-19-26.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Identify Function Area

Question 1
To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections (NIST SP 800-53. Rev. 4: CA-3, PM-5, and CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130)?
Managed and Measurable
The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy. **PASS –** The Gulf Coast Ecosystem Restoration Council (Council) used third party cloud-based systems for all its IT needs, and had only its Office Support Network (OSN) which consisted of a stand-alone group of laptops connected to a leased wireless access point that provided a leased virtual private network connection to the TIC portal, and mobile devices that were not connected to the OSN. As a user (stakeholder) of its information systems, the Council had limited control over its information systems. The Council used eight cloud-based systems and services that were hosted by third parties via interagency agreement. We found the Council ensured that the information systems included in its inventory were subject to the monitoring processes defined within the organization's ISCM strategy.
Optimized
The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near-real time basis. **NOT MET –** Due to the unique size and structure of the Council's information systems, the Council did not use automation to develop a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory was not updated in a near real-time basis.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 2
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2020 CIO FISMA Metrics: 1.2, 1.3, 3.9, CSF: ID.AM-1)?
Managed and Measurable
The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. ***For mobile devices, the agency enforces the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period of time based on agency policy or guidance.*** **PASS –** The Council had no network server and no general support system. Therefore, there were no agency enterprise services for which the Council would have denied access. The Council relied on third party system service providers and only controlled its OSN. In addition to the laptops, the Council used mobile devices that were not connected to the OSN. The Council Chief Information Officer (CIO) tracks and maintains an inventory of its hardware assets and monitors its assets monthly. As the Council had very few IT assets, it was more cost-effective to maintain a list of hardware assets manually.
Optimized
The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization's enterprise architecture current and future states. **NOT MET –** The Council did not employ automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Due to the Council's small organizational size, automated methods for asset management were unnecessary and not cost-effective.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 3
To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?
Managed and Measurable
The organization ensures that the software assets on the network (and their associated licenses) are covered by an organization-wide software asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. ***For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).*** **PASS –** The Council is a micro-agency with stand-alone laptops and mobile devices that were not interconnected. The Council ensured its software assets on the OSN, except mobile devices that were not connected to its OSN, were subject to the monitoring processes defined within the organization's ISCM strategy. The Council users did not have administrator rights to install any software on their laptops. For mobile devices, the Council did not need to enforce the capability to prevent the execution of unauthorized software since they were not connected to the OSN.
Optimized
The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. Further, software inventories are regularly updated as part of the organization's enterprise architecture current and future states. **NOT MET –** We found the Council did not employ automation to track the life cycle of the organization's software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. However, software inventories were regularly updated as part of the organization's enterprise architecture current and future states. It should be noted the Council was a user (stakeholder) of all its information systems. The only software assets the Council was responsible for were the operating system, Microsoft Office, and Adobe software installed on its laptops.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 4
To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?
Consistently Implemented
The organization's defined importance/priority levels for its information systems considers risks from the supporting business functions and mission impacts, including for high value assets, and is used to guide risk management decisions. **PASS –** The Council had a small organization structure without high value assets, and other agencies host and support its cloud-based systems through interagency agreement except the Council's OSN which was managed by the CIO. The third party system service providers were responsible for evaluating the risk to information systems from the supporting business functions and mission impacts.
Managed and Measurable
The organization ensures the risk-based allocation of resources for the protection of high value assets through collaboration and data-driven prioritization. **NOT MET –** The Council did not have high value assets. As such, this maturity level was not applicable to the Council's environment.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 5
To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 – 2; SECURE Technology Act: s. 1326, Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, May 15, 2019)?
Consistently Implemented
The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The organization uses its risk profile to facilitate a determination of the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program. ***In accordance with the SECURE Technology Act, the organization is taking measurable steps to implement its action plan for supply chain risk management.*** **PASS –** The Council consistently implemented its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The Council used its risk profile to facilitate a determination on the aggregate level and types of risk that management was willing to assume. Further, the Council consistently captured and shared lessons learned on the effectiveness of risk management processes and activities to update the program. In addition, the Council addresses supply chain risk management in accordance with the SECURE Technology Act by procuring its assets only from a reputable U.S. company.
Managed and Measurable
The organization monitors and analyzes its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collects, analyzes and reports information on the effectiveness of its risk management program. Data supporting risk management metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** Due to the unique size and structure of the Council's information system, the Council did not monitor and analyze its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and did not collect, analyze, and report information on the effectiveness of its risk management program. Data supporting risk management metrics were not obtained accurately, consistently, and in a reproducible format.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 6
To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?
Consistently Implemented
The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment. ***In addition, the organization employs a software assurance process for mobile applications.*** **PASS –** The Council is a micro-agency with a unique organizational size and structure. The Council relied on third party system service providers and only controlled its OSN which consisted of a stand-alone group of laptops connected to a leased wireless access point that provided a leased virtual private network connection to the TIC portal. The Council relied on third party system service providers to provide security functionality and allocation of security controls. The Council had stand-alone mobile devices that were not connected to the Council's OSN; therefore, they did not employ a software assurance process for mobile applications.
Managed and Measurable
The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems. **NOT MET –** The Council's information security architecture was not integrated with its systems development lifecycle and did not define and direct the implementation of security methods, mechanisms, and capabilities to both the ICT supply chain and its information systems.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 7
To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M-19-03)?
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement risk management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. ***Additionally, the organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.*** **PASS** - The Council had a unique organizational size and structure. The Council CIO was the only employee responsible for all IT related activities. The CIO was intimately involved in all aspects of the Council's risk management program and was aware of every important decision involving its IT operations and its risk management program. The CIO and Deputy Chief Financial Officer communicated to oversee and address the risk management capabilities of the Council. Additionally, the Council had documented the identified risks and developed a defined strategy to mitigate those risks. As such, we determined the maturity level as met based on the above information.
Optimized
The organization's risk management program addresses the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects. **NOT MET** – The Council's risk management program did not address the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects. Due to the unique organizational size and structure of the Council, it may be misleading to state the maturity level of the Council as Optimized.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 8
To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?
Consistently Implemented
The organization consistently utilizes POA&Ms to effectively mitigate security weaknesses. **PASS –** The Council consistently utilized the Plan of Action and Milestones (POA&Ms) to effectively mitigate security weaknesses.
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained. **NOT MET –** Due to the simple network architecture of the Council, and its reliance on the third party system service providers, the Council did not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its POA&M activities and did not use the information to make appropriate adjustments, as needed, to ensure its risk posture was maintained.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 9
To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?
Managed and Measurable
The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. **PASS –** The Council consistently monitored the effectiveness of risk responses to ensure risk tolerances were maintained at an appropriate level.
Optimized
The organization utilizes Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization. **NOT MET** – Due to the simple network architecture of the Council, the Council did not utilize Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization**.**

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 10
To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?
Managed and Measurable
The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of risk. **PASS –** The Council employed robust diagnostic and reporting frameworks, including dashboards which facilitated a portfolio view of interrelated risks across the organization. The dashboards presented qualitative and quantitative metrics that provided indicators of risk.
Optimized
Through the use of risk profiles and dynamic reporting mechanisms, the risk management program provides a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions. **NOT MET –** Due to the unique organizational structure, the Council's risk management program did not provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 11
To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4)?
Consistently Implemented
The organization ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. **PASS –** The Council ensured specific contracting language and service level agreements (SLAs) were consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the Council obtained sufficient assurance that the security controls of systems or services provided by third party service providers met FISMA requirements, OMB policy, and applicable NIST guidance by including specific clauses in its interagency agreements and SLAs.
Managed and Measurable
The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor information security performance of contractor-operated systems and services. **NOT MET –** Because the Council does not own any of its information systems, and does not have any administrative privileges on those systems, the Council does not use qualitative and quantitative performance metrics to measure, report on, and monitor information security performance of contractor-operated systems and services.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 12
To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?
Consistently Implemented
The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of risk information are integrated into the solution. **PASS –** The Council had automated solutions that provided a centralized, enterprise-wide view of risks across the organization, with all necessary sources of risk information integrated.
Managed and Measurable
The organization uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data. **NOT MET –** The Council did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact on organizational systems and data.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management

Question 13
Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?
Question 1 – Maturity Level: Managed and Measurable
Question 2 – Maturity Level: Managed and Measurable
Question 3 – Maturity Level: Managed and Measurable
Question 4 – Maturity Level: Consistently Implemented
Question 5 – Maturity Level: Consistently Implemented
Question 6 – Maturity Level: Consistently Implemented
Question 7 – Maturity Level: Managed and Measurable
Question 8 – Maturity Level: Consistently Implemented
Question 9 – Maturity Level: Managed and Measurable
Question 10 – Maturity Level: Managed and Measurable
Question 11 – Maturity Level: Consistently Implemented
Question 12 – Maturity Level: Consistently Implemented
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and all testing performed in the Risk Management domain, we concluded the Council's overall maturity level for the Risk Management program was Managed and Measurable. Due to the small organizational structure, the Council had the ability to operate more efficiently and effectively compared to larger Federal agencies. The CIO was intimately involved in all aspects of the Council's risk management program and was aware of every important decision involving its IT operations and its risk management program. The Council defined the priority levels for its information systems and considered risks from the supporting business functions and mission impacts to help its leadership make informed risk management decisions. Those informed risk management decisions help to improve and continuously update the Council's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Protect Function Area

Question 14
To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **PASS** – The Council CIO was the lone IT personnel and was directly responsible for managing all information assets in the organization. The Council is a micro-agency with a unique organizational structure. The Council's resources (people, processes, and technology) were allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders were held accountable for carrying out their roles and responsibilities effectively.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 15
To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?
Managed and Measurable
The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. **PASS –** The Council monitored, analyzed, and reported to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, and used this information to take corrective actions when necessary, and ensured data supporting the metrics were obtained accurately, consistently, and in a reproducible format. The Council reviewed the baseline configuration and system component inventory annually. The Council's contractor provided monthly reports to the Council's management that included patch management, hardware, and software scans.
Optimized
The organization utilizes automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization). **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not utilize automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 16
To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: 2.2.1)
Managed and Measurable
The organization monitors, analyzes, and reports on the qualitative and quantitative performance measures used to gauge the effectiveness of its configuration management policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. **PASS –** The Council monitored, analyzed, and reported on the qualitative and quantitative performance measures used to gauge the effectiveness of its configuration management policies and procedures and ensured data supporting the metrics were obtained accurately, consistently, and in a reproducible format. The Council reviewed the baseline configuration and system component inventory annually. The Council's contractor provided monthly reports to the Council's management that included patch management, hardware, and software scans.
Optimized
On a near real-time basis, the organization actively adapts its configuration management plan and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats. **NOT MET –** Due to the unique structure of the Council's information system, the Council did not actively adapt its configuration management plan and related processes on a near real-time basis. We inspected the Council's configuration management plan and determined the plan was reviewed and updated every three years.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 17
To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2020 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?
Managed and Measurable
The organization employs automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact. **PASS –** The Council employed automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and took immediate actions to limit any security impact.
Optimized
The organization utilizes technology to implement a centralized baseline configuration and information system component inventory process that includes information from all organization systems (hardware and software) and is updated in a near real-time basis. **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not utilize technology to implement a centralized baseline configuration and information system component inventory process which included information from all organization systems (hardware and software) and was updated in a near real-time basis.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 18
To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; NIST SP 800-70, Rev. 4, FY 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?
Consistently Implemented
The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes SCAP-validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities. **PASS –** The Council consistently implemented, assessed, and maintained secure configuration settings for its information systems based on the least functionality. Further, the Council consistently utilized Security Content Automation Protocol validated software assessing (scanning) capabilities against all systems on the network to assess and manage both code-based and configuration-based vulnerabilities.
Managed and Measurable
The organization employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network. **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not employ automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the Council's network.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 19
To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?
Managed and Measurable
The organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe. **PASS –** The Council centrally managed its flaw remediation process and utilized automated patch management and software update tools for the operating systems, where such tools were available and safe.
Optimized
The organization utilizes automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe. **NOT MET –** The Council is a small organization that did not have the infrastructure, or the resources needed to automate patch management and software update tools for all applications and network devices.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 20
To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?
Consistently Implemented
The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. ***The agency develops and maintains an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.*** **PASS –** The Council consistently implemented its TIC approved connections and critical capabilities it managed internally. The Council consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure all agency traffic, including mobile and cloud, were routed through defined access points, as appropriate. Furthermore, the Council maintained an accurate inventory of its OSN, including details on its third party service providers.
Managed and Measurable
The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its TIC implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in TIC 3.0, including the use of TIC Use Case requirements, as appropriate, for scenarios in which traffic may not be required to flow through a physical TIC access point. ***Further, the agency has developed a plan to update its internal network and system boundary policies to reflect OMB M-19-26, including guidance regarding TIC Use Case pilots, as appropriate.*** **NOT MET –** The Council implemented TIC initiative per OMB M-19-26 and DHS guidance. However, the Council did not develop a plan to update its internal network and system boundary policies to reflect OMB M-19-26, including guidance regarding TIC Use Case pilots, as appropriate.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 21
To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).
Consistently Implemented
The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation. **PASS –** The Council consistently implemented its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation.
Managed and Measurable
The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council did not monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its change control activities and did not ensure data supporting the metrics was obtained accurately, consistently, and in a reproducible format.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Configuration Management

Question 22
Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
Question 14 – Maturity Level: Managed and Measurable
Question 15 – Maturity Level: Managed and Measurable
Question 16 – Maturity Level: Managed and Measurable
Question 17 – Maturity Level: Managed and Measurable
Question 18 – Maturity Level: Consistently Implemented
Question 19 – Maturity Level: Managed and Measurable
Question 20 – Maturity Level: Consistently Implemented
Question 21 – Maturity Level: Consistently Implemented
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and all testing performed in the Configuration Management domain, we concluded the overall maturity level for the Council's Configuration Management program was Managed and Measurable. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. This allowed the Council to operate more efficiently and effectively than larger organizations because ideas or requests did not need to climb up the levels of management before approval.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 23
To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **PASS –** Due to the Council's organization structure without formal departments and layers of management typically found in larger organizations, we determined that the Council had adequate resources (people, processes, and technology) to consistently implement ICAM activities. Furthermore, we determined that the CIO submitted monthly reports to the senior official of the Council and interacted with the Chief Financial Officer daily to discuss IT issues.
Optimized
In accordance with OMB M-19-17, the agency has implemented an integrated agency-wide ICAM office, team, or other governance structure in support of its ERM capability to effectively govern and enforce ICAM efforts. **NOT MET –** It would not be cost-effective to achieve this maturity level since the Council is a micro-agency with a unique organizational size and structure.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 24
To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM, OMB M-19-17)?
Consistently Implemented
The organization is consistently implementing its ICAM strategy and is on track to meet milestones. The strategy encompasses the entire agency, aligns with the FICAM and CDM requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. **PASS –** The Council consistently implemented its ICAM strategy and was on track to meet milestones.
Managed and Measurable
The organization has transitioned to its desired or "to-be" ICAM architecture and integrates its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture. **NOT MET –** The Council did not have an enterprise architecture like those available in a large organization. The Council relied on third party system service providers and only controlled its OSN which consisted of a stand-alone group of laptops connected to a leased wireless access point that provided a leased virtual private network connection to the TIC portal. Each laptop was a stand-alone with a local user account. A user on laptop 1 could not log into laptop 2 (either locally or over the network) because accounts were only valid to one laptop, so there were no network resources between the laptops. There were no servers on this "network," and as a Windows environment, there was no Active Directory. The wireless access point was only providing a connection out to the Internet to reach hosted resources. As such, the maturity level was Consistently Implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 25
To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17, Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5).
Consistently Implemented
The organization consistently implements its policies and procedures for ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program. The agency ensures that there is regular coordination amongst agency leaders and mission owners to implement, manage, and maintain the agency's ICAM policies, processes, and technologies. **PASS –** The Council consistently implemented its policies and procedures for ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-Council users. Further, the Council consistently captured and shared lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.
Managed and Measurable
The organization uses automated mechanisms (e.g. machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its policies and procedures. Examples of automated mechanisms include network segmentation based on the label/classification of information stored on the servers; automatic removal/disabling of temporary/emergency/ inactive accounts, use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews. **NOT MET –** The Council did not use automated mechanisms (e.g. machine-based, or user-based enforcement) to manage the effective implementation of its policies and procedures. Deployment of automated mechanisms may not be cost-effective considering the structure of the Council environment.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 26
To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?
Consistently Implemented
The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. **PASS –** The CIO was the lone IT personnel and was directly responsible for implementing all identity, credential, and access management activities, including ensuring all new users were assigned an ID and initial passwords to login to their laptops. As his responsibility, the CIO ensured all personnel were assigned risk designations and were appropriately screened prior to being granted access to the system, and rescreened periodically.
Managed and Measurable
The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties. **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not employ automation to centrally document, track, and share risk designations and screening information with necessary parties.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 27
To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?
Consistently Implemented
The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate. **PASS** – The Council had a unique organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for implementing all identity, credential, and access management activities. He ensured access agreements for individuals were completed prior to access being granted to systems and were consistently maintained thereafter. Additionally, there was no sensitive information on the network. As such, the Council did not find it necessary to utilize more specific or detailed agreements. Given the small size of the organization and limited complexity of the IT environment, we determined the Council met the maturity level of Consistently Implemented for this question.
Managed and Measurable
The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized. **NOT MET –** Due to the unique structure of the Council's information systems, the Council did not use automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process was not centralized.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Questions 28
To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2020 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, NIST SP 800-157, and Cybersecurity Sprint)?
Managed and Measurable
All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems. **PASS –** The Council's non-privileged users used strong authentication mechanisms to log into its applicable systems.
Optimized
The organization has implemented an enterprise-wide single sign on the solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis. **NOT MET –** Due to the unique structure of the Council's information systems, an enterprise-wide single sign on solution which can manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require a financial commitment where the cost-benefits may not be justifiable in the Council's environment. As such, the maturity level was Managed and Measurable.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 29
To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; OMB M-19-17, FY 2020 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?
Managed and Measurable
All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems. **PASS –** The Council had a unique organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was assigned a moderate-risk designation. The Council relied on third party system service providers and only controlled its OSN which consisted of a stand-alone group of laptops connected to a leased wireless access point that provided a leased virtual private network connection to the TIC portal. The CIO oversaw all IT infrastructure and privileged user activities. The Council's non-privileged users used strong authentication mechanisms to log into applicable organization systems. Additionally, all privileged and non-privileged users used PIV authentication to login to cloud-based systems. As such, the Council's maturity level was Managed and Measurable.
Optimized
The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis. **NOT MET** - Due to the unique structure of the Council's information systems, an enterprise-wide single sign-on solution which can manage user (privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require a financial commitment where the cost-benefits may not be justifiable in the Council's environment. As such, the maturity level was Managed and Measurable.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 30
To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2020 CIO FISMA Metrics: 2.3, 2.5, and 2.6; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19-01; CSF: PR.AC-4).
Consistently Implemented
The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed. **PASS –** The Council CIO was the lone IT personnel and was directly responsible for implementing all identity, credential, and access management activities. Given the small size of the organization and limited complexity of the IT environment, we determined the Council met the maturity level of Consistently Implemented for this question.
Managed and Measurable
The organization employs automated mechanisms (e.g. machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. **NOT MET –** The Council did not employ automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 31
To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2020 CIO FISMA Metrics: 2.10 and 2.11).
Consistently Implemented
The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk. **PASS –** There were no remote access connections to the Council's OSN. Each laptop had help desk software installed, which allowed a help desk admin to access it when needed. Such a connection was only created when users requested assistance. The help desk employee could only gain access when the user had already logged in to their laptops. The connections used appropriate encryption, and users were automatically logged out after 30 minutes (or less) of inactivity.
Managed and Measurable
The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices. **NOT MET –** The Council is a small organization that did not have the infrastructure, risks, or resources needed to employ processes to ensure end-user devices were appropriately configured prior to allowing remote access and did not restrict the ability of individuals to transfer data accessed remotely to non-authorized devices.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Identity and Access Management

Question 32
Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?
Question 23 – Maturity Level: Managed and Measurable
Question 24 – Maturity Level: Consistently Implemented
Question 25 – Maturity Level: Consistently Implemented
Question 26 – Maturity Level: Consistently Implemented
Question 27 – Maturity Level: Consistently Implemented
Question 28 – Maturity Level: Managed and Measurable
Question 29 – Maturity Level: Managed and Measurable
Question 30 – Maturity Level: Consistently Implemented
Question 31 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and all testing performed in the Identity and Access Management domain, we concluded the overall maturity level for the Council's Identity and Access Management program was Consistently Implemented. Although the maturity level of this domain was Consistently Implemented, our control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Identity and Access Management program controls in place were effective**.** The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no ICAM decisions were made without the CIO's direct involvement and approval. This allowed the Council to operate more efficiently and effectively than larger organizations because ideas or requests did not need to climb up the levels of management before approval.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Data Protection and Privacy

Question 33
To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2019 SAOP FISMA metrics, Sections 1 and 2)?
Consistently Implemented
The organization consistently implements its privacy program by: • ***Dedicating appropriate resources to the program.*** • ***Maintaining an inventory of the collection and use of PII.*** • ***Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems.*** • ***Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs).*** **PASS –** According to the Council's *Privacy Program Plan,* "None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII." The Council staff were trained to not store PII on the laptops or Google Drive. In addition, the CIO performed searches of Google Drive on a quarterly basis to discover and remove any PII. The Council ensured each laptop had encryption enabled on the hard drive.
Managed and Measurable
The organization monitors and analyses quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. The organization conducts an independent review of its privacy program and makes necessary improvements. **NOT MET –** The Council did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and did not use the information to make needed adjustments. Furthermore, the Council did not conduct an independent review of its privacy program and make necessary improvements.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Data Protection and Privacy

Question 34
To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2020 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse
Consistently Implemented
The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data. **PASS –** According to the Council's *Privacy Program Plan,* "None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII." We assessed this maturity level as Consistently Implemented since the Council did not process any form of PII, and this maturity level should not be applicable to the Council's environment.
Managed and Measurable
The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy. **NOT MET –** The Council did not ensure that the security controls for protecting PII throughout the data lifecycle were subject to the monitoring processes since it did not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII information.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Data Protection and Privacy

Question 35
To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2020 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?
Consistently Implemented
The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. ***In addition, the organization utilizes email authentication technology, audits its DNS records, and ensures the use of valid encryption certificates for its domains.*** **PASS –** The Council consistently monitored inbound and outbound network traffic, ensured all traffic passed through a web content filter that protects against phishing, malware, and blocks against known malicious sites. The Council utilized DHS' Continuous Diagnostics and Mitigation Capabilities and EINSTEIN to enhance network defenses. Additionally, the Council checked outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic was quarantined or blocked. As the Council used a third party service provider for email, the third party service provider was responsible for email authentication.
Managed and Measurable
The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. ***Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy.*** **NOT MET –** The Council is a small organization that did not have the infrastructure, risks, or resources needed to analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Data Protection and Privacy

Question 36
To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2019 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?
Consistently Implemented
The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization is able to identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary. **PASS –** The Council did not have network servers to store PII and did not allow PII on the stand-alone laptops. According to the Council's *Privacy Program Plan,* "none of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII." The Council had a Data Breach Response Plan implemented by the CIO, but the Council did not store PII information.
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council is a small organization which did not have the infrastructure, risks, or the resources needed to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan and to obtain data supporting metrics accurately, consistently, and in a reproducible format. As such, we determined this maturity level was not applicable to the Council's environment.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Data Protection and Privacy

Question 37
To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2019 SAOP FISMA Metrics, Sections 9 10, and 11)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)
Consistently Implemented
The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually. **PASS –** The Council ensured all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII received role-based privacy training at least annually. Additionally, the Council ensured individuals certify acceptance of responsibilities for privacy requirements at least annually.
Managed and Measurable
The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing. **NOT MET –** The Council updated its training program based on statutory, regulatory, mission, program, business process, information system requirements. However, the Council did not utilize feedback on the content of its training. As such, we determined that the Council did not meet this maturity level.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Data Protection and Privacy

Question 38
Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?
Question 33 – Maturity Level: Consistently Implemented
Question 34 – Maturity Level: Consistently Implemented
Question 35 – Maturity Level: Consistently Implemented
Question 36 – Maturity Level: Consistently Implemented
Question 37 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and all testing performed in the Data Protection and Privacy domain, we concluded the overall maturity level for the Council's Data Protection and Privacy program was Consistently Implemented. Although the maturity level of this domain was Consistently Implemented, our control testing for this domain found no exceptions, and the controls were operating as intended. We concluded the Council's Data Protection and Privacy program controls in place were effective**.** Due to the small organizational size and limited internal IT systems, the duties of positions were very limited, and multiple roles and responsibilities were accomplished by both the CIO and Chief Financial Officer. The agency did not process any PII data. PII data needed for human resources and payroll were handled through agreements with a Federal Shared Service Provider whose systems were approved to collect and process PII data. It should be noted, due to the unique organizational structure of the Council, some of the areas which determine the maturity level of the Council's Data Protection and Privacy domain may not be applicable.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 39
To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **PASS -** The Council had a unique organizational structure with the CIO as the only person responsible for all day-to-day activities of the Council's IT security awareness and training program. As a result, we determined resources were allocated in a risk-based manner as the CIO was the lone IT personnel in the organization.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 40
To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?
Managed and Measurable
The organization has addressed its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors. **PASS –** The Council addressed its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors. The CIO stated additional hiring of staff/contractors was unnecessary to maintain needed knowledge, skills, and abilities. Based on our understanding of the small size of the organization, and the limited scope of the IT environment, we determined the Council met the maturity level of Managed and Measurable for this question.
Optimized
The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time. **NOT MET –** No security incidents occurred at the Council during the FISMA year. If any incidents happened on the systems managed through interagency agreements, the Council would be notified by the third party system service providers. As such, we could not determine that the Council's personnel collectively possessed a training level such that the Council could demonstrate security incidents resulting from personnel actions or inactions were being reduced over time.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 41
To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **PASS –** The Council monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The Council ensured data supporting metrics were obtained accurately, consistently, and in a reproducible format. The CIO reviewed all results of testing and made updates to quarterly training based on the analysis as applicable.
Optimized
The organization's security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program. **NOT MET –** The Council did not integrate security awareness and training activities across other security-related domains. For instance, common risks, control weaknesses, and other outputs of the agency's risk management and continuous monitoring activities did not inform any updates which need to be made to the security awareness and training program.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 42
To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **PASS –** The Council monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The Council ensured data supporting metrics were obtained accurately, consistently, and in a reproducible format.
Optimized
On a near real-time basis, the organization actively adapts its security awareness and training policies, procedures, and program to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats. **NOT MET –** On a near real-time basis, the Council did not actively adapt its security awareness and training policies, procedures, and programs to a changing cybersecurity landscape.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 43
To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2020 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).
Consistently Implemented
The organization ensures that all systems users complete the organization's security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements. **PASS –** The Council ensured all systems users completed its security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintained completion records. The Council obtained feedback on its security awareness and training program and used the information to make improvements.
Managed and Measurable
The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. **NOT MET –** As a small organization with limited IT infrastructure, the Council did not have much exposure to risk. While the Council conducted phishing awareness training, we did not receive enough evidence to validate a phishing exercise was performed to measure the effectiveness of the training.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 44
To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?
Consistently Implemented
The organization ensures that individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records. **PASS –** The Council ensured individuals with significant security responsibilities were provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintained appropriate records.
Managed and Measurable
The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. **NOT MET –** The Council is a small organization and did not measure the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The Council conducted phishing awareness training but did not perform phishing exercises.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Security Training

Question 45
Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?
Question 39 – Maturity Level: Managed and Measurable
Question 40 – Maturity Level: Managed and Measurable
Question 41 – Maturity Level: Managed and Measurable
Question 42 – Maturity Level: Managed and Measurable
Question 43 – Maturity Level: Consistently Implemented
Question 44 – Maturity Level: Consistently Implemented
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and all testing performed in the Security Training domain, we concluded the overall maturity level for the Council's Security Training program was Managed and Measurable. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT security training.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ISCM

Detect Function Area

Question 46
To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **PASS –** The Council relied on third party service providers for its ISCM capabilities. The third party service providers monitored and analyzed measures on the effectiveness of the Council's ISCM policies and procedures. The Council reviewed reports provided by the third party service providers to better ascertain the effectiveness of its ISCM policies and procedures.
Optimized
The organization's ISCM strategy is fully integrated with its risk management, configuration management, incident response, and business continuity functions. **NOT MET –** The Council did not fully integrate its ISCM strategy with risk management, configuration management, incident response, and business continuity functions.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ISCM

Question 47
To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **PASS –** The Council relied on third party service providers for its ISCM capabilities. The third party service providers monitored and analyzed measures on the effectiveness of the Council's ISCM policies and procedures. The Council reviewed reports provided by the third party service providers to better ascertain the effectiveness of its ISCM policies and procedures.
Optimized
The organization's ISCM policies and procedures are fully integrated with its risk management, configuration management, incident response, and business continuity functions. **NOT MET –** The Council's ISCM policies and procedures were not fully integrated with its risk management, configuration management, incident response, and business continuity functions.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ISCM

Question 48
To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1)?
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **PASS –** The Council had a small organization structure without the typical network available in a large organization, and the CIO was the lone IT personnel. The Council relied on third party service providers to manage its information systems. As such, the Council's service providers were responsible for implementing ISCM activities on those systems. It would be inaccurate to state the Council does not meet the Managed and Measurable maturity level.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ISCM

Question 49
How mature are the organization's processes for performing ongoing assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls (OMB A-130, NIST SP 800-137: Section 2.2; NIST SP 800-53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NIST SP 800-18, Rev. 1, NISTIR 8011; OMB M-14-03; OMB M-19-03)
Optimized
The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **PASS –** The Council had a simple, flat organizational structure without formal departments and layers of management. The direct involvement of the CIO and leadership allowed the Council to achieve cost-effective IT security objectives and goals which helped facilitate decision-making and minimized cost, risk, and impact on the Council's mission.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ISCM

Question 50
How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?
Optimized
On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **PASS –** On a near real-time basis, the small organizational structure and size enabled the Council to actively adapt its ISCM program to a changing cybersecurity landscape and respond to evolving and sophisticated threats in a timely manner.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ISCM

Question 51
Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?
Question 46 – Maturity Level: Managed and Measurable
Question 47 – Maturity Level: Managed and Measurable
Question 48 – Maturity Level: Managed and Measurable
Question 49 – Maturity Level: Optimized
Question 50 – Maturity Level: Optimized
OVERALL: Managed and Measurable
Based on the maturity levels generated from the questions and the testing performed in the ISCM domain, we concluded the overall maturity level of the Council's ISCM program was Managed and Measurable. The Council's simple, flat organizational structure, which did not have any formal departments or layers of management, allowed the Council to operate more efficiently and effectively than larger organizations. Decisions regarding IT operations were made with the direct involvement and approval of the Council's CIO allowing the leadership to easily monitor and analyze qualitative and quantitative performance measures across the organization and the effectiveness of its ISCM program. The direct involvement of the CIO and leadership allowed the Council to achieve cost-effective IT security objectives and goals which helped facilitate decision-making and minimize cost, risk, and impact on the Council's mission.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Respond Function Area

Question 52
To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-19-03; FY 2020 CIO FISMA Metrics, Section 4; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).
Consistently Implemented
The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy and processes to update the program. **PASS –** No incidents occurred at the Council during the FISMA year. As such, there were no means to verify the implementation of the Council's incident response policies, procedures, plans, and strategies. However, it would be inaccurate to state the Council had not met the Consistently Implemented maturity level.
Managed and Measurable
The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** No incidents occurred at the Council during the FISMA year. As such, we could not determine the effectiveness of this maturity level.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 53
To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-20-04; FY 2020 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?
Consistently Implemented
Individuals are performing the roles and responsibilities that have been defined across the organization. **PASS –** We interviewed the Council CIO and inspected the Council's organizational documents and determined that individuals performed the roles and responsibilities which were defined across the Council.
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **NOT MET –** Due to the small organizational structure of the Council, and its reliance on third party service providers which gives the Council limited exposure to the possibility of security incidents, the Council only had part-time incident response team members, serving as more of a virtual incident response team. As such, we could not determine if resources were allocated in a risk-based manner for shareholders to implement incident response activities.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 54
How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS-8; and US-CERT Incident Response Guidelines)?
Consistently Implemented
The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software. **PASS –** The Council is a small organization without a typical network available in a large organization. All Council information systems, except the OSN, were managed by third party service providers. As such, the service providers were responsible for implementing processes for incident detection, analysis, and prioritization. In addition, the service providers were responsible for utilizing technologies such as intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.
Managed and Measurable
The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems. **NOT MET –** The Council is a small organization without the typical network available in a large organization, and the Council relied on third party service providers to manage its information systems. We were unable to verify if the Council's service providers utilize profiling techniques to measure the characteristics of expected activities on its networks and systems so it can more effectively detect security incidents.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 55
How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)?
Managed and Measurable
The organization manages and measures the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability. **PASS –** As a small-agency which primarily uses information system hosted by third party providers, the Council had limited exposure to vulnerabilities and security incidents on its information systems. The Council had not experienced any incidents during the FISMA year, and the size of the agency should enable it to respond to any incidents timely.
Optimized
The organization utilizes dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems. **NOT MET –** The Council is a micro-agency that primarily used information systems hosted by third party providers. The use of dynamic reconfiguration to stop attacks, misdirect attackers, and to isolate components of systems may be burdensome due to the Council's organizational structure.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 56
To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)?
Consistently Implemented
The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner. **PASS –** The Council had a simple, flat organizational structure, without formal departments or layers of management like larger organizations. No incidents occurred at the Council during the FISMA year. As such, there were no means to verify information regarding sharing information on incident activities and reporting incidents in a timely manner. However, it would be inaccurate to state the Council had not met the Consistently Implemented maturity level because they have processes and controls in place for incidents that start with the anti-virus software, patches, a help desk with problem escalation processes, and continuous monitoring.
Managed and Measurable
Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. **NOT MET –** It should be noted as the Council is a small organization without the typical IT infrastructures available in a larger organization, the agency had limited exposure to incidents and its information systems were managed by third parties. We found no evidence that the Council's incident response metrics were used to measure and manage the timely reporting of incident information to its officials and external stakeholders since no incident occurred on the Council system during the FISMA year.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 57
To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41)?
Managed and Measurable
The organization utilizes Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises. **PASS –** The Council utilized EINSTEIN 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 58
To what degree does the organization utilize the following technology to support its incident response program? • Web application protections, such as web application firewalls • Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools • Aggregation and analysis, such as security information and event management (SIEM) products • Malware detection, such as antivirus and antispam software technologies • Information management, such as data loss prevention • File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)
Managed and Measurable
The organization uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. **PASS –** The Council did not use these technologies since it relied on its service providers. Therefore, we determined this maturity level was not applicable to the Council's environment. However, the Council's third party service providers used technologies for monitoring and analyzing qualitative and quantitative performance across the organization and collected, analyzed, and reported data on the effectiveness of its technologies for performing incident response activities. Therefore, we determined the Council's maturity level as Managed and Measurable for this metric.
Optimized
The organization has institutionalized the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation-based technologies to continuously determine the impact of potential security incidents to its IT assets) and adjusts incident response processes and security measures accordingly. **NOT MET –** The Council did not institutionalize the implementation of advanced incident response technologies for analysis of trends and performance against benchmarks (e.g., simulation-based technologies to continuously determine the impact of potential security incidents to its IT assets) and did not adjust its incident response processes and security measures accordingly.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Incident Response

Question 59
Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?
Question 52 – Maturity Level: Consistently Implemented
Question 53 – Maturity Level: Consistently Implemented
Question 54 – Maturity Level: Consistently Implemented
Question 55 – Maturity Level: Managed and Measurable
Question 56 – Maturity Level: Consistently Implemented
Question 57 – Maturity Level: Managed and Measurable
Question 58 – Maturity Level: Managed and Measurable
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and the testing performed in the Incident Response domain, we concluded the overall maturity level of the Council's Incident Response program was Consistently Implemented. Since the Council did not own any servers or general support systems, and they depended on third party providers, the Council had limited exposure to the possibility of security incidents and only had part-time incident response team members who served more as a virtual incident response team. The small organizational structure enabled the Council to respond to and address security incidents promptly. As a result, the Council's Computer Security Incident Response Center could be assembled quickly to meet the required reporting timelines and help the Council expedite reporting of incidents that could help serve to mitigate or prevent damage to the Council's information systems.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Recover Function Area

Question 60
To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?
Managed and Measurable
Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. **PASS** - The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval.
Optimized
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 61
To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800-161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5, FY 2020 CIO FISMA Metrics, Section 5)?
Consistently Implemented
The organization consistently implements its defined information system contingency planning policies, procedures, and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program. **PASS –** The Council consistently implemented its defined information systems contingency planning policies, procedures, and strategies. The Council owned only their OSN and depended on third party providers for all other services. The Council consistently captured and shared lessons learned on the effectiveness of information systems contingency planning policies, procedures, strategy, and processes to update the program.
Managed and Measurable
The organization understands and manages its information and communications technology (ICT) supply chain risks related to contingency planning activities. As appropriate, the organization: integrates ICT supply chain concerns into its contingency planning policies and procedures, defines and implements a contingency plan for its ICT supply chain infrastructure, applies appropriate ICT supply chain controls to alternate storage and processing sites, considers alternate telecommunication service providers for its ICT supply chain infrastructure and to support critical information systems. **NOT MET –** The Council had a unique organizational structure and size. However, we noted the Council did not integrate ICT supply chain concerns into the contingency planning policies and procedures. As such, the maturity level was Consistently Implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 62
To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-19-03; FY 2020 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?
Consistently Implemented
The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets. **PASS –** The Council is a small organization and does not have the typical network available in larger organizations that may require an organizational and system-level Business Impact Analysis (BIA). The Council's cloud-based systems, except the OSN, were managed by third party service providers; however, the Council's CIO created a BIA for the OSN.
Managed and Measurable
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 63
To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2020 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?
Consistently Implemented
Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans. **PASS –** The Council is a small organization which relied on third party service providers to manage its information systems, except for the OSN managed by the CIO, and the Council had developed an Information Systems Contingency Plan for its OSN. The plan considered activation and notification, recovery, and reconstitution. Each system managed by the service provider received a FISMA certification ensuring it complied with contingency plans and NIST guidelines were met.
Managed and Measurable
The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization. **NOT MET –** The Council did not integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans. The Council owned few IT assets and had contracts with third party service providers for its information processing needs and therefore did not have integrated metrics on the effectiveness of those information system contingency plans as the third parties had the responsibility to do so.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 64
To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2020 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?
Consistently Implemented
Processes for information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP. **PASS –** Processes for information system contingency plan testing and exercises were consistently implemented. Information Systems Contingency Plan testing and exercises were integrated, to the extent practicable, with testing of related plans.
Managed and Measurable
The organization employs automated mechanisms to more thoroughly and effectively test system contingency plans. ***In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.*** **NOT MET –** The Council is a small organization that did not have the infrastructure, risks, or resources needed to manage and employ automated mechanisms to more thoroughly and effectively test system contingency plans.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 65
To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2020 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?
Consistently Implemented
The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized and are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained. **PASS –** Though the Council defined the processes, strategies, and technology for information system backup and storage, the Council did not have a typical network as found in larger organizations. Given the small size of the organization, limited complexity of the IT environment, the fact the Council's information systems were managed by third parties and were therefore not subjected to the same physical and cybersecurity risks, we determined the Council met the maturity level of Consistently Implemented for this question. In addition, we examined each of the service provider's SLAs and determined they addressed contingency planning or continuity of operations.
Managed and Measurable
Per the FISMA Reporting Metrics, this maturity level was not applicable to this question.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 66
To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?
Consistently Implemented
Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk-based decisions. **PASS –** The Council had a small organizational structure without a typical network available in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. The Council did not experience any incidents, therefore there was no evidence of any recovery activities performed.
Managed and Measurable
Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format. **NOT MET –** The Council did not experience any incidents, and no recovery activities were performed. As such, we assessed the maturity level as Consistently Implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Contingency Planning

Question 67
Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?
Question 60 – Maturity Level: Managed and Measurable
Question 61 – Maturity Level: Consistently Implemented
Question 62 – Maturity Level: Consistently Implemented
Question 63 – Maturity Level: Consistently Implemented
Question 64 – Maturity Level: Consistently Implemented
Question 65 – Maturity Level: Consistently Implemented
Question 66 – Maturity Level: Consistently Implemented
OVERALL: Consistently Implemented
Based on the maturity levels generated from the questions and the testing performed in the Contingency Planning domain, we concluded the overall maturity level of the Council's Contingency Planning program was Consistently Implemented. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. The CIO's direct control allowed the Council to operate more efficiently and effectively than larger organizations because ideas or requests did not need to climb up the levels of management before approval.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Appendix II: Management Response

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Gulf Coast Ecosystem Restoration Council

October 14, 2020

Richard K. Delmar
Deputy Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Room4436
Washington, DC 20220

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2020

Thank you for the opportunity to review The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2020.

The Council agrees with the report that Council's information security program and practices were effective for the period July 1, 2019 through June 30, 2020. The Council works to ensure that its information assurance program meets the key performance areas for the five cybersecurity framework security functions that make up the 67 FISMA reporting metrics issued by the Department of Homeland Security (DHS).

In fiscal year 2021 the Council will use this evaluation report to inform its information assurance decisions to ensure a continued effective information security program. The Council will also continue its efforts to consistently implement, manage and measure its IT security program at an optimized level in order to support projects and programs to achieve the goals and objectives of the RESTORE Act for restoration in the Gulf Coast region.

Sincerely,

Ben Scaggs
Executive Director
Gulf Coast Ecosystem Restoration Council

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline:
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
http://www.treasury.gov/about/organizational-structure/ig