Evaluation Report

OIG-CA-19-005

INFORMATION TECHNOLOGY: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2018

October 24, 2018

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 24, 2018

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 2018*

We are pleased to transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2018*, dated October 23, 2018. 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 (DHS) 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, 2017 through June 30, 2018. 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 5 Cybersecurity Functions and 8 FISMA Metric Domains. RMA found that the Council's information security program and practices were effective for the period July 1, 2017 through June 30, 2018.

Appendix I of the attached RMA report includes the *FY 2018 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 210
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 2018

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

October 23, 2018

The Honorable Eric Thorson
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 2018

Dear Mr. Thorson:

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 2018. 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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1* (May 24, 2018) 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, 2017 through June 30, 2018.

In summary, we found that the Council's information security program and practices were effective for the period July 1, 2017 through June 30, 2018.

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

The Gulf Coast Ecosystem Restoration Council
Federal Information Security Modernization Act of 2014
Evaluation Report for Fiscal Year 2018

Table of Contents

ABBREVIATIONS

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
OMB	Office of Management and Budget
OSN	Office Support Network
PII	Personally Identifiable Information
RESTORE Act	Resources and Ecosystems Sustainability, Tourist Opportunities, and Revived Economies of the Gulf Coast States Act of 2012
SP	Special Publications
TIC	Trusted Internet Connection

INTRODUCTION

This report presents the results of our independent evaluation of the Gulf Coast Ecosystem Restoration Council (Council)'s information systems' security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA) requires Federal agencies to have an annual independent evaluation performed of their information security program and practices 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 Department of Homeland Security (DHS) for the collection of annual FISMA responses. DHS prepared the FISMA questionnaire to collect these responses, which is provided in Appendix I: *FY 2018 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 that the agency Inspector General (IG) or an independent external auditor, as determined by the IG, perform the annual evaluation. The Department of the Treasury Office of Inspector General engaged RMA Associates, LLC to conduct an evaluation in support of the FISMA requirement for an annual evaluation of the Council's information security program and practices. The objective of this evaluation was to evaluate the effectiveness of the Council's information security program and practices for the period July 1, 2017 through June 30, 2018.

This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency 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 function areas to be addressed in the independent assessment of agencies' information security programs. See *Objective, Scope, and Methodology* for more detail.

SUMMARY EVALUATION RESULTS

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 have been maintained for the 5 Cybersecurity Functions[1] and 8 FISMA Metric Domains.[2] We found that the Council's information security program and practices were effective for the period July 1, 2017 through June 30, 2018.

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.

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. The 8 FISMA Metric Domains were aligned with the 5 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 DHS' FISMA Reporting Metrics, the 8 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.

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 Gulf Coast Ecosystem Restoration Council (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 has few information technology (IT) assets and only 22 employees. 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.

The system service providers support the Council's major applications:

1. For payroll processing, the Council uses WebTA hosted by the National Finance Center.
2. For financial management and reporting processing, the Council uses the Department of the Treasury Bureau of the Fiscal Service's Administrative Resource Center (ARC).
3. For grants processing, the Council uses the Restoration Assistance and Awards Management System (RAAMS) hosted by the U.S. Geological Survey.
4. For website support, the Council uses U.S. Geological Survey hosting services.

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, requires 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 of 2014 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, strengthens the use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused 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 thereafter.

These management responsibilities presume that responsible agency officials understand the risks and other factors that 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 in order to make informed judgments and investments that 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 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 that 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 were not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies were formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies were 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 were collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies were fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The answers to the 67 FISMA Reporting Metrics in Appendix 1 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 included questions pertaining to Risk Management and Contractor systems;
- Protect, which included questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, which included questions pertaining to Information Security Continuous Monitoring;
- Respond, which included questions pertaining to Incident Response; and
- Recover, which included 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. We considered that the Chief Information Officer (CIO) is closely involved in all aspects of the Council's IT environment and is 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 maturity level for each of the domains, 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 computers 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 as Managed and Measurable. The Council defined the priority levels for its IT 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 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 as Managed and Measurable. Since 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 26 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.

Identity and Access Management: We determined the Council's overall maturity level for the Identity and Access Management program as Consistently Implemented. The Council had 22 employees to manage their Identity, Credential, and Access Management (ICAM) protocols. While policies and procedures were consistently implemented, the Council did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews 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 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 as Consistently Implemented. The Council did not process

Personally Identifiable Information (PII) data, as PII data needed for human resources and payroll was handled through agreements with a Federal Shared Service Provider whose systems were approved to collect and process PII data. While policies and procedures were consistently implemented, the Council did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and use that information to make needed adjustments that were necessary to reach the Managed and Measurable level. Our testing of PII controls 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 as Managed and Measurable. The Council had 22 employees, and our testing of employees' security awareness and role-based training found no exceptions. 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 as Managed and Measurable. Decisions regarding IT operations were made with the direct involvement and approval of the Council's CIO, allowing the 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 as Consistently Implemented. Since 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 quickly respond and address security incidents. 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. In addition, the Council executed a Memorandum of Agreement with DHS's Office of Cybersecurity and Communications to utilizes DHS' EINSTEIN intrusion prevention security services. Our testing found no exceptions and the controls were operating as intended. 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 as Consistently Implemented. Since the Council did not own any network servers and did not have a general support system, it developed policies and procedures for Contingency Planning that were consistently implemented, but did not develop quantitative and qualitative effectiveness measures that were necessary to reach the Managed and Measurable level. Our testing 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 that, 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 have been maintained for the 5 Cybersecurity Functions and 8 FISMA Metric

Domains. We found that the Council's information security program and practices were effective for the period July 1, 2017 through June 30, 2018.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this evaluation was to determine the effectiveness of the Council's information security program and practices for the period July 1, 2017 through June 30, 2018.

Scope

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. The evaluation was designed to determine whether the Council implemented selected security controls for selected information systems in support of the *Federal Information Security Modernization Act of 2014*. Our evaluation was conducted for the period between July 1, 2017 and June 30, 2018. It consisted of testing the 67 FISMA Reporting Metrics issued by DHS.

Methodology

Our overall strategy of our evaluation considered *NIST 800-53A, Guide for Assessing Security Controls in Federal Information Systems and Organizations, NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*, and the FISMA guidance from CIGIE, OMB, and DHS. 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 Special Publication (SP) 800-53A. 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, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. Also, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However, in cases where we did not select the entire evaluation population, the results were not projected.

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 2018 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

NIST Federal Information Processing Standards (FIPS) and SPs

- 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, *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*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, *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, *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, *Digital Identity Guidelines*
- NIST SP 800-83, *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, *NICE Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-17-09, *FY 2017 Management of Federal High-Value Assets*
- OMB Memorandum M-16-04, *FY 2016 Cybersecurity Strategy and Implementation Plan (CISP) for the Federal Civilian Government*
- OMB Memorandum M-14-03, *FY 2014 Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-08-05, *FY 2008 Implementation of Trusted Internet Connections (TIC)*
- OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
- OMB Circular A-130, *Managing Information as a Strategic Resource*

Department of Homeland Security

- *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1 May 24, 2018*

Appendix I: *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*

IDENTIFY FUNCTION AREA

Table 3: Risk Management

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: CA-3, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1 and 1.4)?
Managed and Measurable
The organization ensures that the information systems included in its inventory were subject to the monitoring processes defined within the organization's ISCM strategy. **Pass –** 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 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 –** The Council did not use automation to develop a centralized information system inventory that included hardware and software components from all organizational information systems. The centralized inventory was not updated in a near real-time basis.

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 connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics: 1.2)?
Managed and Measurable
The organization ensures that the hardware assets connected to the network were subject to the monitoring processes defined within the organization's ISCM strategy. **Pass –** The Council ensured that the hardware assets connected to the network were subject to the monitoring processes defined within the organization's ISCM strategy.
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 were 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.

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: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?
Managed and Measurable
The organization ensures that the software assets on the network (and their associated licenses) were subject to the monitoring processes defined within the organization's ISCM strategy. **Pass –** The Council ensured its software assets on the network (and their associated licenses) were subject to the monitoring processes defined within the organization’s ISCM strategy.
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 were 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 software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management.

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 (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?
Consistently Implemented
The organization's defined importance/priority levels for its information systems considers risks from the supporting business functions and mission impacts and is used to guide risk management decisions. **Pass –** The Council's defined importance/priority levels for its information systems considered risks from the supporting business functions and mission impacts and was used to guide risk management decisions.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Risk Management

Question 5
To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that 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: 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)?
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 on 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. **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.
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 were obtained accurately, consistently, and in a reproducible format. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources needed to collect, monitor, analyze and report qualitative and quantitative performance measures. Collecting data supporting the risk management program is a manual process and it not part of a periodic, consistent, automated reproducible process.
Optimized
The enterprise risk management program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and capital planning and investment control. Further, the organization's risk management program is embedded into daily decision making across the organization and provides for continuous risk identification. **Not Met –** The enterprise risk management program is a manual process and not integrated with other security areas, and other business processes, such as strategic planning and capital planning and investment control.

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 (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA- 12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?
Consistently Implemented
The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews were consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment. **Pass –** The Council consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews were consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment.
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 organization's information security architecture was not 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.
Optimized
The organization uses advanced technologies and techniques for managing supply chain risks. To the extent practicable, the organization is able to quickly adapt its information security and enterprise architectures to mitigate supply chain risks. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources needed for a defined information security architecture that is integrated with its systems development lifecycle. The Council does not own applications that are subject to application change management process and the ICT supply chain**.**

Risk Management

Question 7
To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?
Managed and Measurable
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 utilized an integrated risk management governance structure for implementing and overseeing an enterprise risk management capability that managed risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.
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.

Risk Management

Question 8
To what extent has the organization ensured that plans of action and milestones (POA&Ms) were utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?
Consistently Implemented
The organization consistently utilizes POA&Ms to effectively mitigate security weaknesses. **Pass –** The Council consistently utilized plan of action and milestones 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 –** The Council is a small organization that did not have the infrastructure or the resources needed to collect, monitor, analyze and report qualitative and quantitative performance measures of its plan of action and milestones activities.
Optimized
The organization employs automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions in a near real-time basis. Furthermore, processes were in place to identify and manage emerging risks, in addition to known security weaknesses. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources needed to employ automation to correlate security weaknesses amongst information systems and identify enterprise-wide trends and solutions in a near real-time basis.

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 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?
Managed and Measurable
The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances were maintained at an appropriate level. **Pass –** The Council consistently monitored the effectiveness of risk responses to ensure that risk tolerances were maintained at an appropriate level.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Risk Management

Question 10
To what extent does the organization ensure that information about risks were 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))?
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 that facilitated a portfolio view of interrelated risks across the organization. The dashboard 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 –** The risk management program did not provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.

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 (FAR Case 2007- 004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?
Consistently Implemented
The organization ensures that specific contracting language and SLAs were consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance 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 that specific contracting language and Service Level Agreements 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 contractors or other entities on behalf of the Council meet FISMA requirements, OMB policy, and applicable NIST guidance.
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 –** The Council is a small organization that did not have the infrastructure or the resources needed to collect, monitor, analyze and report qualitative and quantitative performance measures of contractor-operated systems and services.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

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 were integrated into the solution. **Pass –** The Council consistently implemented an automated solution across the enterprise that provided 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 were integrated into the solution.
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 is a small organization that did not have the infrastructure or the resources needed to automate performances of scenario analysis and model potential responses that includes modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems.
Optimized
The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its risk management program. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources needed to institutionalize the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its risk management program.

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, we found that the controls were effective.

Questions	Maturity Level
1	Managed and Measurable
2	Managed and Measurable
3	Managed and Measurable
4	Consistently Implemented
5	Consistently Implemented
6	Consistently Implemented
7	Managed and Measurable
8	Consistently Implemented
9	Managed and Measurable
10	Managed and Measurable
11	Consistently Implemented
12	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 determined the Council's overall maturity level for the Risk Management program as **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 considers 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 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.

PROTECT FUNCTION AREA

Table 4: Configuration Management

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: CM-1; NIST SP 800-128: Section 2.4)?
Consistently Implemented
Stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities. **Pass –** Stakeholders had adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Configuration Management

Question 15
To what extent does the organization utilize an enterprise-wide configuration management plan that included, 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: 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 that data supporting the metrics was obtained accurately, consistently, and in a reproducible format.
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 –** 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).

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: 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 that data supporting the metrics was obtained accurately, consistently, and in a reproducible format.
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 –** The Council did not, on a near real-time basis, actively adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats.

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: CM-2 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?
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 –** The Council did not utilize technology to implement a centralized baseline configuration and information system component inventory process that included information from all organization systems (hardware and software) and was updated in a near real-time basis.

Configuration Management

Question 18
To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?
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. **Pass –** The Council employed 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.
Optimized
The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis. **Not Met –** The Council did not deploy system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis.

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: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?
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 were available and safe. **Pass –** The Council centrally managed its flaw remediation process and utilized automated patch management and software update tools for 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, as appropriate, where such tools were 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.

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-08-05)?
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, were routed through defined access points, as appropriate. **Pass –** The Council consistently implemented its TIC approved connections and critical capabilities that it manages internally. The Council consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure that all agency traffic, including mobile and cloud, were routed through defined access points, as appropriate.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

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 were 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: CM-2 and CM-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 is a small organization that did not have the infrastructure or the resources needed to monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its change control activities.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

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, we found that the controls were effective.

Questions	Maturity Level
14	Consistently Implemented
15	Managed and Measurable
16	Managed and Measurable
17	Managed and Measurable
18	Managed and Measurable
19	Managed and Measurable
20	Consistently Implemented
21	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 determined the overall maturity level for the Council's Configuration Management program as **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 to monitor all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. This allows the Council to operate more efficiently and effectively than larger organizations because ideas or requests do not need to climb up the levels of management before approval.

Identity and Access Management

Table 5: 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: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?
Consistently Implemented
Stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities. **Pass –** Stakeholders had adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Identity and Access Management

Question 24
To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?
Consistently Implemented
The organization is consistently implementing its ICAM strategy and is on track to meet milestones. **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 is a small organization that did not have the infrastructure or the resources needed to develop a transition plan to its desired or "to-be" ICAM architecture and integrates its ICAM strategy and activities.
Optimized
On a near real-time basis, the organization actively adapts its ICAM strategy and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources needed to monitor on a near real-time basis, actively adapt its ICAM strategy and related processes and activities to a changing cybersecurity landscape to respond to evolving and sophisticated threats.

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: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1).
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 nonorganizational 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. **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 is a small organization that did not have the infrastructure or the resources needed to implement automated mechanisms (e.g. machine-based, or user-based enforcement) to manage the effective implementation of its policies and procedures.
Optimized
The organization employs adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near real-time basis. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources needed to implement adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near real-time basis.

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: PS-2 and PS- 3; National Insider Threat Policy)?
Consistently Implemented
The organization ensures that all personnel were assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. **Pass –** The Council ensured that all personnel were assigned risk designations, appropriately screened prior to being granted system access, 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 –** The Council is a small organization that did not have the infrastructure or the resources needed to implement automation to centrally document, track, and share risk designations and screening information with necessary parties.
Optimized
On a near-real-time basis, the organization evaluates personnel security information from various sources, integrates this information with anomalous user behavior data (audit logging) and/or its insider threat activities, and adjusts permissions accordingly. **Not Met –** The Council is a small organization that did not have the infrastructure or the resources need to on a near-real-time basis, evaluate personnel security information from various sources, integrate this information with anomalous user behavior data (audit logging) and/or its insider threat activities, and adjust permissions accordingly.

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 were completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

Consistently Implemented

The organization ensures that access agreements for individuals were completed prior to access being granted to systems and were 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 ensured that access agreements for individuals were completed prior to access being granted to systems and were consistently maintained thereafter. The Council utilized more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

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 – The Council is a small organization that did not have the infrastructure or the resources needed to automate manage and review user access agreements for privileged and non-privileged users.

Optimized

On a near real-time basis, the organization ensures that access agreements for privileged and nonprivileged users were maintained, as necessary.

Not Met – The Council is a small organization that did not have the infrastructure or the resources needed to on a near real-time basis, ensure that access agreements for privileged and nonprivileged users were maintained, as necessary.

Identity and Access Management

Questions 28
To what extent has the organization implemented strong authentication mechanisms (two factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?
Consistently Implemented
The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets. **Pass –** The Council consistently implemented strong authentication mechanisms for non-privileged users of the Council's facilities and networks, including for remote access, in accordance with Federal targets.
Managed and Measurable
All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to utilize strong authentication mechanisms to authenticate all non-privileged users.
Optimized
The organization has implemented an enterprise-wide single sign-on solution and all 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 –** The Council is a small organization that did not have the infrastructure, risks or the resources needed implement an enterprise-wide single sign-on solution that results in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.

Identity and Access Management

Question 29
To what extent has the organization implemented strong authentication mechanisms (two factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?
Consistently Implemented
The organization has consistently implemented strong authentication mechanisms for privileged users of the organization’s facilities and networks, including for remote access, in accordance with Federal targets. **Pass –** The Council consistently implemented strong authentication mechanisms for privileged users of the Council’s facilities and networks, including for remote access, in accordance with Federal targets.
Managed and Measurable
All privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to implement strong authentication mechanisms to authenticate to all privileged users.
Optimized
The organization has implemented an enterprise-wide single sign-on solution and all 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 –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed implement an enterprise-wide single sign-on solution that results in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.

Identity and Access Management

Question 30
To what extent does the organization ensure that privileged accounts were 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 were logged and periodically reviewed (FY 2018 CIO FISMA Metrics: 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP).
Consistently Implemented
The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts were 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 were logged and periodically reviewed. **Pass –** The Council ensured that its processes for provisioning, managing, and reviewing privileged accounts were consistently implemented across the Council. The Council limited the functions that could be performed when using privileged accounts; limited the duration that privileged accounts could be logged in; limited the privileged functions that could be performed using remote access; and ensured that privileged user activities were logged and periodically reviewed.
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 is a small organization that did not have the infrastructure, risks, or the resources needed to employ automated mechanisms to support the management of privileged accounts.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Identity and Access Management

Question 31
To what extent does the organization ensure that appropriate configuration/connection requirements were 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: AC17 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10).
Consistently Implemented
The organization ensures that FIPS 140-2 validated cryptographic modules were implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities were logged and reviewed based on risk. **Pass –** The Council ensured that FIPS 140-2 validated cryptographic modules were implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities were logged and reviewed based on risk.
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 nonauthorized devices. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to employ processes to ensure 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 nonauthorized devices.
Optimized
The organization has deployed a capability to rapidly disconnect remote access user sessions based on active monitoring. The speed of disablement varies based on the criticality of missions/business functions. **Not Met –** The Council has not deployed a capability to rapidly disconnect remote access user sessions based on active monitoring. The speed of disablement varies based on the criticality of missions/business functions.

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, our testing found that the controls were effective.

Questions	Maturity Level
23	Consistently Implemented
24	Consistently Implemented
25	Consistently Implemented
26	Consistently Implemented
27	Consistently Implemented
28	Consistently Implemented
29	Consistently Implemented
30	Consistently Implemented
31	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 determined the overall maturity level for the Council's Identity and Access Management program as **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 is the lone IT personnel and was directly responsible to monitor all IT assets. Further, no ICAM decisions were made without the CIO's direct involvement and approval. This allows 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.

Data Protection and Privacy

Table 6: Data Protection and Privacy

Question 33
To what extent had the organization developed a privacy program for the protection of personally identifiable information (PII) that was collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?
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, and reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs) **Pass –** The Council consistently implemented 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, and reviewing and removing unnecessary PII collections on a regular basis (i.e., Social Security Numbers).
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 is a small organization that did not have the infrastructure, risks or the resources needed to monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities.
Optimized
The privacy program is fully integrated with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management. Further, the organization's privacy program is embedded into daily decision making across the organization and provides for continuous identification of privacy risks. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to fully integrate the privacy program with other security areas, such as ISCM, and other business processes, such as strategic planning and risk management.

Data Protection and Privacy

Question 34

To what extent had 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; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10, and 2.12)?

- 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 – The Council's policies and procedures were 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.

Managed and Measurable

The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle were subject to the monitoring processes defined within the organization's ISCM strategy.

Not Met – The Council is a small organization that did not have the infrastructure, risks, or the resources needed to implement security controls for protecting PII and other agency sensitive data, throughout the data lifecycle and implement a monitoring processes defined within the organization's ISCM strategy.

Optimized

The organization employs advanced capabilities to enhance protective controls, including (i) remote wiping, (ii) dual authorization for sanitization of media devices, (iii) exemption of media marking as long as the media remains within organizationally-defined control areas, and (iv) configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule.

Not Met – The Council is a small organization that did not have the infrastructure, risks, or the resources needed employ advanced capabilities to enhance protective controls, including (i) remote wiping, (ii) dual authorization for sanitization of media devices, (iii) exemption of media marking as long as the media remains within organizationally-defined control areas, and (iv) configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule.

Data Protection and Privacy

Question 35
To what extent had the organization implemented security controls to prevent data exfiltration and enhance network defenses (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.10)?
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. **Pass –** The Council consistently monitored inbound and outbound network traffic, ensuring that all traffic passed through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization 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.
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. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The Council is a small organization that did not have the infrastructure, risks or the resources needed to conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.
Optimized
The organization's data exfiltration and enhanced network defenses were fully integrated into the ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to enhance data exfiltration and enhanced network defenses and integrate them into the ISCM and incident response programs to provide near real-time monitoring of the data that was entering and exiting the network, and other suspicious inbound and outbound communications.

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: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; 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 consistently implemented its Data Breach Response plan. Additionally, the breach response team participated in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization was 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.
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 were obtained accurately, consistently, and in a reproducible format. **Not Met –** The Council is a small organization that 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 the infrastructure, risks or the resources needed to obtain data supporting metrics accurately, consistently, and in a reproducible format.
Optimized
The organization's Data Breach Response plan is fully integrated with incident response, risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Further, the organization employs automation to monitor for potential privacy incidents and takes immediate action to mitigate the incident and provide protection to the affected individuals. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to fully integrate with incident response, risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate.

Data Protection and Privacy

Question 37
To what degree does the organization ensure that privacy awareness training was provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (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 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 ensured that 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 is a small organization that did not have the infrastructure, risks, or the resources needed to measure 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.
Optimized
The organization has institutionalized a process of continuous improvement incorporating advanced privacy training practices and technologies. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to institutionalize a process of continuous improvement incorporating advanced privacy training practices and technologies

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, we found that the controls were effective.

Questions	Maturity Level
33	Consistently Implemented
34	Consistently Implemented
35	Consistently Implemented
36	Consistently Implemented
37	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 determined the overall maturity level for the Council's Data Protection and Privacy program as **Consistently Implemented.** 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 the Chief Financial Officer. The agency did not process any PII data. PII data needed for human resources and payroll was handled through agreements with a Federal Shared Service Provider whose systems were approved to collect and process PII data. It should be noted that due to the unique organizational structure of the Council, some of the areas that determine the maturity level of the Council's Data Protection and Privacy domain may not be applicable. According to the Council's *Incident Response Procedures*, "none of The Council Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII."

Security Training

Table 7: 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 included 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 80053: AT-1; and NIST SP 800-50).
Consistently Implemented
Roles and responsibilities for stakeholders involved in the organization's security awareness and training program have been defined and communicated across the organization. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities. **Pass –** Roles and responsibilities for stakeholders involved in the Council's security awareness and training program were defined and communicated across the Council. In addition, stakeholders had adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

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: 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.
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 were being reduced over time. **Not Met –** The Council's personnel did not collectively possess a training level such that the organization could demonstrate that security incidents resulting from personnel actions or inactions were being reduced over time.

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 was 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: AT-1; NIST SP 800-50: Section 3).]
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 were obtained accurately, consistently, and in a reproducible format. **Pass –** The Council did monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The Council ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.
Optimized
The organization's security awareness and training activities were integrated across other security-related domains. For instance, common risks, 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.

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: 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 were obtained accurately, consistently, and in a reproducible format. **Pass –** The Council did monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The Council ensures that 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 –** The Council did not, on a near real-time basis, actively adapts its security awareness and training policies, procedures, and program to a changing cybersecurity landscape.

Security Training

Question 43

To what degree does the organization ensure that security awareness training was provided to all system users and was 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: AT- 2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; 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 that all systems users complete the Council's 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 that 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 – The Council is a small organization that did not have the infrastructure, risks, or the resources needed to measure the effectiveness of its awareness training program.

Optimized

The organization has institutionalized a process of continuous improvement incorporating advanced security awareness practices and technologies.

Not Met – The Council is a small organization that did not have the infrastructure, risks, or the resources needed to institutionalize a process of continuous improvement incorporating advanced security awareness practices and technologies.

Security Training

Question 44

To what degree does the organization ensure that specialized security training was provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Consistently Implemented

The organization ensures that individuals with significant security responsibilities were provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records.

Pass – The Council ensured that 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 that did not have the infrastructure, risks, or the resources needed to obtain feedback on its security training content and makes updates to its program. In addition, The Council is a small organization that did not have the infrastructure, risks or the resources needed to 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**.**

Optimized

The organization has institutionalized a process of continuous improvement incorporating advanced security training practices and technologies.

Not Met – The Council is a small organization that did not have the infrastructure, risks, or the resources needed to institutionalize a process of continuous improvement incorporating advanced security training practices and technologies.

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, we found that the controls were effective.

Questions	Maturity Level
39	Consistently Implemented
40	Managed and Measurable
41	Managed and Measurable
42	Managed and Measurable
43	Consistently Implemented
44	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 determined the overall maturity level for the Council's Security Training program as **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 to monitor all IT security training.

ISCM

DETECT FUNCTION AREA

Table 8: ISCM

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 800-137: Sections 3.1 and 3.6)?
Consistently Implemented
The organization's ISCM strategy is consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy. **Pass –** The Council’s ISCM strategy was consistently implemented at the organization, business process, and information system levels. In addition, the strategy supported clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captured lessons learned to make improvements to the ISCM strategy.
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 were obtained accurately, consistently, and in a reproducible format. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM strategy.
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 is a small organization that did not have the infrastructure, risks or the resources needed to fully integrated with its risk management, configuration management, incident response, and business continuity functions.

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: CA-7) (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 were obtained accurately, consistently, and in a reproducible format. **Pass –** The Council monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and made updates, as appropriate. The Council ensured that data supporting metrics were obtained accurately, consistently, and in a reproducible format.
Optimized
The organization's ISCM policies and procedures were fully integrated with its risk management, configuration management, incident response, and business continuity functions. **Not Met –** The Council did not fully integrate ISCM policies and procedures with risk management, configuration management, incident response, and business continuity functions.

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: CA-1; NIST SP 800-137)?
Managed and Measurable
The organization's staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the organization's ISCM program. **Pass –** The Council's staff consistently collected, monitored, and analyzed qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the organization's ISCM program.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

ISCM

Question 49
How mature were the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800- 53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?
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 ISCM program achieves cost-effective IT security objectives and goals and influences decision-making that is based on cost, risk, and mission impact.

ISCM

Question 50
How mature was 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 organization actively adapted its ISCM program to a changing cybersecurity landscape.

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, we found that the controls were effective.

Questions	Maturity Level
46	Consistently Implemented
47	Managed and Measurable
48	Managed and Measurable
49	Optimized
50	Optimized
OVERALL	**Managed and Measurable**

Based on the maturity levels generated from the questions and the testing performed in the ISCM domain, we determined the overall maturity level of the Council's ISCM program as **Managed and Measurable.** The Council's simple and flat organizational structure which did not have any formal departments or layers of management allows 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 allows the Council to achieve cost-effective IT security objectives and goals that help to facilitate the decision-making and minimize cost, risk, and impact on the Council's mission.

Incident Response

RESPOND FUNCTION AREA

Table 9: Incident Response

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: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics:4.2; 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 –** The Council consistently implemented its incident response policies, procedures, plans, and strategies. Further, the Council consistently captured and shared lessons learned on the effectiveness of its incident response policies, procedures, strategy, and processes to update the program.
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 were obtained accurately, consistently, and in a reproducible format. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate.
Optimized
The organization's incident response program, policies, procedures, strategies, plans with related activities were fully integrated with risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Not Met –** The Council is a small organization that did not have the infrastructure, risks or the resources needed to fully integrated with risk management with continuous monitoring, continuity of operations, and other mission/business areas.

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: IR-7; NIST SP 800- 83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: 4.1-4.3; and US-CERT Federal Incident Notification Guidelines)?
Consistently Implemented
Defined roles and responsibilities were consistently implemented, and teams have adequate resources (people, processes, and technology) to consistently implement incident response activities. **Pass –** Defined roles and responsibilities were consistently implemented, and teams had adequate resources (people, processes, and technology) to consistently implement incident response activities.
Managed and Measurable
The organization has assigned responsibility for monitoring and tracking the effectiveness of incident response activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of incident response activities. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of incident response activities.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Incident Response

Question 54
How mature were 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-18-02; 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 consistently utilized its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the Council implemented and analyzed precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management, 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 were 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 that did not have the infrastructure, risks, or the resources needed to use profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Incident Response

Question 55
How mature were the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?
Consistently Implemented
The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations. **Pass –** The Council consistently implemented its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may were exploited on the target system(s), and recovers system operations.
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 were not subject to exploitation of the same vulnerability. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to manage and measure the impact of successful incidents and quickly mitigate related vulnerabilities so that they were not subject to exploitation of the same vulnerability. The Council has contract with AGJ Systems & Networks, Inc to monitor for security incidents.
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 small organization that did not have the infrastructure, risks, or the resources needed to utilize 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.

Incident Response

Question 56
To what extent does the organization ensure that incident response information was shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800- 53: IR-6; US-CERT Incident Notification Guidelines; PPD- 41; 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 were reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner. **Pass –** The Council consistently shared information on incident activities with internal stakeholders. The Council ensured that security incidents were reported to United States Computer Emergency Readiness Team, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner.
Managed and Measurable
Incident response metrics were used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to timely manage and measure incident response and report incidents to organizational officials and external stakeholders.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

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: IR-4; OMB M-18-02; 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
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Incident Response

Question 58

To what degree does the organization utilize the following technology to support its incident response program?

- Web application protection, 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 used 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.

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 has not 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).

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, we found that the controls were effective.

Questions	Maturity Level
52	Consistently Implemented
53	Consistently Implemented
54	Consistently Implemented
55	Consistently Implemented
56	Consistently Implemented
57	Managed and Measurable
58	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 determined the overall maturity level of the Council's Incident Response program as **Consistently Implemented.** Since the Council did not own any servers or general support systems, the Council had limited exposure to the possibility of security incidents and only had part-time incident response team members who serve more as a virtual incident response team. The small organizational structure enables the Council to quickly respond and address security incidents. As a result, the Council's Computer Security Incident Response Center can be assembled quickly to meet the required reporting timelines and help the Council expedite reporting of incidents which can help serve to mitigate or prevent damage to the Council's information systems.

Contingency Planning

RECOVER FUNCTION AREA

Table 10: Contingency Planning

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: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?
Consistently Implemented
The organization has established appropriate teams that were ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities. **Pass –** The Council established appropriate teams that were ready to implement its information system contingency planning strategies. Stakeholders and teams had adequate resources (people, processes, and technology) to effectively implement system contingency planning activities.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Contingency Planning

Question 61
To what extent had 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)
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 system contingency planning policies, procedures, and strategies. The Council did not own any information systems, as they depend on third-party providers. The Council consistently captured and shared lessons learned on the effectiveness of information system 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 does not have an information and communications technology (ICT) supply chain.
Optimized
The information system contingency planning program is fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization. **Not Met –** The Council did not have an integrated enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization.

Contingency Planning

Question 62
To what degree does the organization ensure that the results of business impact analyses were used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.1)?
Consistently Implemented
The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System-level BIAs were 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 were consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets. **Pass –** The Council incorporated the results of organizational and system level Business Impact Analyses (BIA) into strategy and plan development efforts. System-level BIAs were integrated with the organizational level BIA and included 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 were consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Contingency Planning

Question 63
To what extent does the organization ensure that information system contingency plans were developed, maintained, and integrated with other continuity plans (NIST SP 800-53: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1)?
Consistently Implemented
Information system contingency plans were 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 were 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 –** Information system contingency plans were consistently developed and implemented for systems and included organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities were integrated with other continuity areas including Council and business process continuity, disaster recovery planning, incident management, insider threat implementation plan, and occupant emergency plans.
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 owns few IT assets and contracts with third-party service providers for its information processing needs and did not have integrated metrics on the effectiveness of its information system contingency plans as the third parties have the responsibility to do so.
Optimized
Information system contingency planning activities were fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas and embedded into daily decision making across the organization. **Not Met –** Information system contingency planning activities were not fully integrated with the enterprise risk management program, strategic planning processes, capital allocation/budgeting, and other mission/business areas.

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: CP-3 and CP-4)?
Consistently Implemented
Processes for information system contingency plan testing and exercises were 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 System 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. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to manage employ automated mechanisms to more thoroughly and effectively test system contingency plans.
Optimized
The organization coordinates information system contingency plan testing with organizational elements responsible for related plans. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate. **Not Met –** The Council did not coordinate information system contingency plan testing with organizational elements responsible for related plans.

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: 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; 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 were chosen based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized and were 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 were configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system levels were consistently performed, and the confidentiality, integrity, and availability of this information is maintained. **Pass –** The Council consistently implemented its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites. The Council depended upon third-party service providers to provide backup.
Managed and Measurable
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

Contingency Planning

Question 66
To what level does the organization ensure that information on the planning and performance of recovery activities was communicated to internal stakeholders and executive management teams and used to make risk-based decisions (CSF: RC.CO-3; NIST SP 800-53: 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 –** Information on the planning and performance of recovery activities was consistently communicated to relevant stakeholders and executive management teams, who utilized the information to make risk-based decisions.
Managed and Measurable
Metrics on the effectiveness of recovery activities were communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. **Not Met –** The Council is a small organization that did not have the infrastructure, risks, or the resources needed to manage metrics on the effectiveness of recovery activities and to communicate the metrics to relevant stakeholders.
Optimized
N/A – per the FISMA Reporting Metrics, this maturity level is not applicable for this question.

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, we found that the controls were effective.

Questions	Maturity Level
60	Consistently Implemented
61	Consistently Implemented
62	Consistently Implemented
63	Consistently Implemented
64	Consistently Implemented
65	Consistently Implemented
66	Consistently Implemented
OVERALL	**Consistently Implemented**

Based on the maturity levels generated from the questions and the testing performed in the Incident Response domain, we determined the overall maturity level of the Council's Contingency Planning program as **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 to monitor all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. This allows the Council to operate more efficiently and effectively than larger organizations because ideas or requests do not need to climb up the levels of management before approval.

Appendix II: MANAGEMENT RESPONSE

Gulf Coast Ecosystem Restoration Council

October 5, 2018

RMA Associates, LLC
1005 N. Glebe Road, Suite 210
Arlington, Virginia 22201

Re: Gulf Coast Ecosystem Restoration Council (Council) Federal Information Security Modernization Act of 2014 Fiscal Year 2018 Evaluation

Gentlemen:

In response to the Council Federal Information Security Modernization Act of 2014 Fiscal Year 2018 Evaluation, the Council agrees with the report that 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 and eight FISMA Metric Domains, and that the Council's information security program and practices were effective for the period of July 1, 2017 through June 30, 2018. The Council appreciates the courtesy and professionalism extended by the audit team and by the Office of Inspector General.

In fiscal year 2019 the Council will 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.

Ben Scaggs

Ben Scaggs
Executive Director

REPORT WASTE, FRAUD, AND ABUSE

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

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

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