



# Evaluation Report



OIG-CA-20-006

INFORMATION TECHNOLOGY: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2019

October 25, 2019

Office of  
Inspector General

Department of the Treasury

**This Page Intentionally Left Blank**



OFFICE OF  
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

October 25, 2019

**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 2019*

The purpose of this memorandum is to transmit the attached report, *The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2019*, dated October 25, 2019. 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, 2018 through June 30, 2019. 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, 2018 through June 30, 2019.

Appendix I of the attached RMA report includes the *FY 2019 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

**The Gulf Coast Ecosystem Restoration Council  
Federal Information Security Modernization Act of 2014  
Evaluation Report for Fiscal Year 2019**

October 25, 2019

Richard K. Delmar  
Acting 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 2019

Dear Mr. Delmar:

RMA Associates, LLC is pleased to submit the Gulf Coast Ecosystem Restoration Council (Council) Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2019. 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3* (April 9, 2019) 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, 2018 through June 30, 2019.

In summary, we found that the Council's information security program and practices were effective for the period July 1, 2018 through June 30, 2019.

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 2019**

**Table of Contents**

**ABBREVIATIONS** ..... *ii*

**INTRODUCTION**..... *1*

**SUMMARY EVALUATION RESULTS**..... *1*

**BACKGROUND**..... *2*

**OBJECTIVE, SCOPE, AND METHODOLOGY**..... *8*

**CRITERIA**..... *10*

**Appendix I: FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics**..... *13*

**KEY CHANGES TO THE FY 2019 IG FISMA METRICS**..... *14*

**IDENTIFY FUNCTION AREA**..... *15*

**PROTECT FUNCTION AREA**..... *28*

**DETECT FUNCTION AREA**..... *60*

**RESPOND FUNCTION AREA**..... *66*

**RECOVER FUNCTION AREA**..... *74*

**Appendix II: Management Response**..... *82*

## 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
SDLC	Systems Development Life Cycle
NARA	National Archives and Records Administration
SCAP	Security Content Automation Protocol



## 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 the 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 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FISMA Reporting Metrics). We also considered applicable OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines.

FISMA requires the agency Inspector General (IG) or an independent external auditor, as determined by the IG, to perform the annual evaluation. The Department of the Treasury 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, 2018, through June 30, 2019.

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

## SUMMARY EVALUATION RESULTS

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<sup>1</sup> and eight FISMA Metric Domains.<sup>2</sup> The overall maturity level of the Council's information security program was determined as Managed and Measurable, as described in this report. Accordingly, we found that the Council's information security program and practices were effective for the period July 1, 2018 through June 30, 2019.

---

<sup>1</sup> 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*.

<sup>2</sup> As described in 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.

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

## **BACKGROUND**

### **Gulf Coast Ecosystem Restoration Council**

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

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

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

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 report processing, the Council uses the Treasury'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; expected to be replaced in FY 2020.
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, strengthened use of continuous monitoring in systems, and 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 after that.

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 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.

Our evaluation was conducted for the period between July 1, 2018, and June 30, 2019. It consisted of testing the 67 FISMA Reporting Metrics listed in the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* Version 1.3 (April 9, 2019) issued by DHS. 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. The Council did not change IT controls, processes, personnel, or systems since the prior year's FISMA evaluation. 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 is 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 that 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 is 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 their laptops. Our testing found no exceptions, and the controls were operating as intended. We concluded that 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 is Consistently Implemented. The Council had to manage the Identity, Credential, and Access Management (ICAM) protocols for approximately 30 employees and contractors. 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 that 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 is Consistently Implemented. The Council did not process Personally Identifiable Information (PII) data as PII data needed for human resources and payroll were handled through agreements with a Federal Shared Service Provider whose systems were approved to collect and process PII data. 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. 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.

**Security Training:** We determined the Council's overall maturity level for the Security Training program is Managed and Measurable. The Council had approximately 30 employees and contractors, 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 is 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 is 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 respond and address security incidents quickly. As a result, the Council's Computer Security Incident Response Center could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. In addition, the Council executed a Memorandum of Agreement with DHS' Office of Cybersecurity and Communications to utilize DHS' EINSTEIN intrusion prevention security services. 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.

**Contingency Planning:** We determined the Council's overall maturity level for the Contingency Planning program is 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. 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 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 the Council's information security program and practices were effective for the period July 1, 2018, through June 30, 2019, and the overall maturity level of the Council's information security program is Managed and Measurable.

## OBJECTIVE, SCOPE, AND METHODOLOGY

### Objective and Scope

The objective of this evaluation was to determine the effectiveness of the Gulf Coast Ecosystem Restoration Council (Council)'s information security program and practices for the period of July 1, 2018 through June 30, 2019.

RMA determined the effectiveness of the Council's overall information technology (IT) security program and practices by evaluating the following five Cybersecurity Framework security functions (key performance areas) outlined in the annual *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3 April 9, 2019* (FISMA Reporting Metrics):

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

The FISMA evaluation was designed to determine whether the Council implemented selected security controls on its information systems in support of the *Federal Information Security Modernization Act of 2014*. We tested all of the Council's information systems including the Council's in-house Office Support Network (OSN) and third-party service providers systems of WebTA, Administrative Resource Center (ARC), Restoration Assistance and Awards Management System (RAAMS), and the Council's website. Our evaluation was conducted for the period between July 1, 2018, and June 30, 2019. It consisted of testing the 67 FISMA Reporting Metrics issued by the Department of Homeland Security (DHS).

We conducted the FISMA evaluation in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*, issued January 2012, and subsequent revisions, the Office of Management and Budget<sup>3</sup> (OMB) and the Department of

---

<sup>3</sup> OMB Circular No. A-130, "Managing Information as a Strategic Resource"; and OMB Memorandum 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2018.



Homeland Security<sup>4</sup> most recent FISMA reporting guidance, FISMA Reporting Metrics, the National Institute of Standards and Technology (NIST) guidance,<sup>5</sup> and policies and procedures from the Council.

## Methodology

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

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

In testing for the effectiveness of the security controls, 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.

---

<sup>4</sup> Homeland Security Federal Information Security Memorandum (FISMA) 14-01, *Fiscal Year 2014 Metrics for the Federal Information Security Management Act of 2002 and Agency Privacy Management Act and Operational Reporting Instructions*.

<sup>5</sup> NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations (April 2013)*; and National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity version 1.1 dated April 16, 2018*.

## CRITERIA

We focused our *Federal Information Security Modernization Act of 2014* (FISMA) evaluation approach on Federal information security guidelines developed by the Gulf Coast Ecosystem Restoration Council (Council), National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB). National Institute of Standards and Technology Special Publications (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 2019 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-PI-Security Planning Policy and Procedures
- GCC-IT-19-RA-Risk Assessment Procedures
- GCC-IT-20-CC-Security Assessment and Authorization Procedures
- GCC-IT-21-SC Security Assessment and Authorization
- GCC-IT-22-SI System and Information Integrity Procedures
- GCC-IT-23-SA-System and Services Acquisitions
- GCC-IT-24-Mobile Device Policy
- GCC-IT-25-Mobile Code Technologies
- GCC-IT-26-Sanitization Procedures

### NIST Federal Information Processing Standards (FIPS) and Special Publications

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*

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

### **OMB Policy Directives**

- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*
- OMB Circular A-130, *Managing Information as a Strategic Resource*

## Department of Homeland Security

- *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3 April 9, 2019*

***Appendix I: FY 2019 Inspector General Federal Information Security Modernization Act of  
2014 Reporting Metrics***

## KEY CHANGES TO THE FY 2019 IG FISMA METRICS

The Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2018<sup>6</sup> (SECURE Technology Act) established new requirements for supply chain risk management. The *FY 2019 IG FISMA Reporting Metrics* have been updated to gauge agencies' preparedness in addressing these new requirements while recognizing that specific guidance will be issued at a later date.

In addition, since the publication of the *FY 2018 IG FISMA Reporting Metrics*, the National Institute of Standards and Technology (NIST) updated several of its Special Publications (SP) to enhance existing criteria, such as NIST SP 800-37 (Revision 2) and NIST SP 800-160 (Volume 1). These updates include changes to criteria that impact the *FY 2019 IG FISMA Reporting Metrics*, such as an alignment with the constructs in the NIST Cybersecurity Framework, the integration of privacy risk management processes, alignment with system life cycle security engineering processes, and the incorporation of supply chain risk management processes. While the updates will not go into full effect until one year after their respective publications, the criteria references in the *FY 2019 IG FISMA Reporting Metrics* have been updated to reflect these changes.

---

<sup>6</sup> Public Law No: 115-390 (December 21, 2018).

**Risk Management**

**IDENTIFY FUNCTION AREA**

**Table 3: Risk Management**

Question 1
<p>To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections (NIST SP 800- 53. Rev. 4: CA-3, PM-5, and CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130)?</p>
<b>Managed and Measurable</b>
<p><i>The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy</i></p> <p><b>PASS</b> – The Council uses third-party systems for all its information systems, and as a user (stakeholder) of its information systems, the Council has limited control of its information systems. The Council has four information systems and were most effectively managed by third-party via interagency agreement. We found the Council ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization’s ISCM strategy. The Council subjected information systems included in its inventory to the monitoring processes.</p>
<b>Optimized</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – Due to the unique structure of the Council’s information systems, 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.</p>

**Risk Management**

<b>Question 2</b>
<p>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 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1)?</p>
<b>Managed and Measurable</b>
<p><i>The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.</i></p> <p><b>PASS</b> – The Council has no network server and no general support systems. The Council has stand-alone workstations with a Trusted Internet Connection (TIC) to shared service providers. Since they have very few IT assets, it is more cost-effective to maintain a list of hardware assets manually.</p>
<b>Optimized</b>
<p><i>The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization’s enterprise architecture current and future states.</i></p> <p><b>NOT MET</b> – The Council did not employ automation to track the life cycle of the organization’s hardware assets with processes that limit the manual/procedural methods for asset management. Due to the Council’s small organizational size, automated methods for asset management is unnecessary and not cost-effective.</p>



**Risk Management**

<b>Question 3</b>
<p>To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?</p>
<b>Managed and Measurable</b>
<p><i>The organization ensures that the software assets on the network (and their associated licenses) are covered by an organization-wide software asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.</i></p> <p><b>PASS</b> – 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.</p>
<b>Optimized</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – We found the Council does not employ automation to track the life cycle of the organization’s software assets (and their associated licenses) with processes that limit the manual/procedural methods for asset management. However, software inventories are regularly updated as part of the organization’s enterprise architecture current and future states. It should be noted that the Council is a user (stakeholder) of all its information systems. The only software assets the Council is responsible for are the operating system (OS) and software installed on its workstations.</p>

**Risk Management**

<b>Question 4</b>
<p>To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?</p>
<b>Consistently Implemented</b>
<p><i>The organization’s defined importance/priority levels for its information systems considers risks from the supporting business functions and mission impacts, including for high-value assets, and is used to guide risk management decisions.</i></p> <p><b>PASS</b> – The Council has a small organization structure, and other agencies manage all its information systems through interagency agreement except the Council’s Office Support Network (OSN) which is managed by the CIO. The third-party providers will be responsible for evaluating the risk to information systems from the supporting business functions and mission impacts. We inquired of CIO whether the Council has high value assets, the Council informed us they do not possess any high-value assets.</p>
<b>Managed and Measurable</b>
<p><i>The organization ensures the risk-based allocation of resources for the protection of high value assets through collaboration and data-driven prioritization.</i></p> <p><b>NOT MET</b> – We inquired of the Council CIO to understand whether the Council holds any high value assets, we were informed, the Council does not have high value assets. As such, this maturity level is not applicable to the Council’s environment.</p>

**Risk Management**

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

## 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; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

#### Consistently Implemented

*The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment.*

**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 before 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 ICT supply chain and the organization's information systems.

**Risk Management**

<b>Question 7</b>
<p>To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M19-03)?</p>
<b>Managed and Measurable</b>
<p><i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement risk management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. Additionally, the organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.</i></p>
<p><b>PASS</b> -The Council has a unique organizational structure and size. The Council Chief Information Officer (CIO) is the only employee with privileged access to the organization's Office Support Network (OSN). He is responsible for all IT-related activities. The CIO is intimately involved in all aspects of the Council's risk management program and is aware of every important decision involving its IT operations and its risk management program. The CIO and Senior Accountable Official for Risk Management communicate with each other to oversee and address the risk management capabilities of the Council. As such, we determined the maturity level as met based on the above information.</p>
<b>Optimized</b>
<p><i>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.</i></p>
<p><b>NOT MET</b> – Due to the unique organizational structure and size, the Council's risk management program did not address the full spectrum of the agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects.</p>

**Risk Management**

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

## Risk Management

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

**Risk Management**

Question 10
<p>To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?</p>
Managed and Measurable
<p><i>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.</i></p> <p><b>PASS</b> – 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.</p>
Optimized
<p><i>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.</i></p> <p><b>NOT MET</b> – Due to the unique organizational structure, the Council’s risk management program did not provide a fully integrated, prioritized, enterprise-wide view of organizational risks to drive strategic and business decisions.</p>



**Risk Management**

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

**Risk Management**

<b>Question 12</b>
<p>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)?</p>
<b>Consistently Implemented</b>
<p><i>The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of risk information are integrated into the solution.</i></p> <p><b>PASS</b> – 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.</p>
<b>Managed and Measurable</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – The Council did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data.</p>

**Risk Management**

**Question 13**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?*

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
<b>OVERALL</b>	<b>Managed and Measurable</b>

Based on the maturity levels generated from the questions and all testing performed in the Risk Management domain, we concluded that the Council’s overall maturity level for the Risk Management program is **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 improve continually 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.

**Configuration Management**

**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 REV. 4: CM-1; NIST SP 800- 128: Section 2.4)?
Managed and Measurable
<i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.</i>
<b>PASS</b> – The Council CIO is the lone IT personnel and is directly responsible for managing all information assets in the organization. The Council is a micro-agency with a unique organizational structure. The Council’s resources (people, processes, and technology) were allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.
Optimized
Per the <i>FY 2019 IG FISMA Reporting Metrics</i> , this maturity level does not apply to this question.

## Configuration Management

Question 15
<p>To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization’s System Development Life Cycle (SDLC); configuration monitoring; and applying configuration management requirements to contractor-operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?</p>
Managed and Measurable
<p><i>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.</i></p> <p><b>PASS</b> – 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 were obtained accurately, consistently, and in a reproducible format.</p>
Optimized
<p><i>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)</i></p> <p><b>NOT MET</b> – Due to the unique structure of the Council’s information systems, the Council did not utilize automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis (as defined by the organization).</p>

**Configuration Management**

<b>Question 16</b>
<p>To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM1; NIST SP 800-128: 2.2.1)</p>
<b>Managed and Measurable</b>
<p><i>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.</i></p> <p><b>PASS</b> – 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 were obtained accurately, consistently, and in a reproducible format.</p>
<b>Optimized</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – Due to the unique structure of the Council’s information systems, the Council did not actively adapt its configuration management plan and related processes on a near real-time basis. We inspected the Council’s configuration management plan and determined the plan is reviewed and updated every three years.</p>

**Configuration Management**

Question 17
<p>To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM8; FY 2019 CIO FISMA Metrics: 1.1, 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?</p>
Managed and Measurable
<p><i>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.</i></p> <p><b>PASS</b> – 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.</p>
Optimized
<p><i>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.</i></p> <p><b>NOT MET</b> – Due to the unique structure of the Council’s information systems, the Council did not utilize technology to implement a centralized baseline configuration and information system component inventory process that included information from all organization systems (hardware and software) and was updated in a near real-time basis.</p>

**Configuration Management**

<b>Question 18</b>
<p>To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; FY 2019 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?</p>
<b>Consistently Implemented</b>
<p><i>The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes Security Content Automation Protocol (SCAP) validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities.</i></p> <p><b>PASS</b> – The Council consistently implemented, assessed, and maintained secure configuration settings for its information systems based on the least functionality. Further, the Council consistently utilizes SCAP validated software assessing (scanning) capabilities against all systems on the network to assess and manage both code-based and configuration-based vulnerabilities.</p>
<b>Managed and Measurable</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – Due to the unique structure of the Council’s information systems, the Council did not employ automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the Council’s network.</p>



**Configuration Management**

<b>Question 19</b>
<p>To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2019 CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?</p>
<b>Managed and Measurable</b>
<p><i>The organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.</i></p> <p><b>PASS</b> – 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.</p>
<b>Optimized</b>
<p><i>The organization utilizes automated patch management and software update tools for all applications and network devices, as appropriate, where such tools are available and safe.</i></p> <p><b>NOT MET</b> – 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.</p>

## 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)?
<b>Consistently Implemented</b>
<i>The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.</i>
<b>PASS</b> – 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.
<b>Managed and Measurable</b>
Per the <i>FY 2019 IG FISMA Reporting Metrics</i> , this maturity level does not apply to this question.

**Configuration Management**

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

**Configuration Management**

**Question 22**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?*

Questions	Maturity Level
14	Managed and Measurable
15	Managed and Measurable
16	Managed and Measurable
17	Managed and Measurable
18	Consistently Implemented
19	Managed and Measurable
20	Consistently Implemented
21	Consistently Implemented
<b>OVERALL</b>	<b>Managed and Measurable</b>

Based on the maturity levels generated from the questions and all testing performed in the Configuration Management domain, we concluded that the overall maturity level for the Council’s Configuration Management program is **Managed and Measurable**. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO’s direct involvement and approval. This 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
<p>To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?</p>
<b>Consistently Implemented</b>
<p><i>Individuals are performing the roles and responsibilities that have been defined across the organization.</i></p> <p><b>PASS</b> – We determined that individuals are performing the roles and responsibilities that have been defined across the organization.</p>
<b>Managed and Measurable</b>
<p><i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.</i></p> <p><b>NOT MET</b> - Due to the Council’s organization structure with a limited scope of IT environment, we determined that the Council has adequate resources (people, processes, and technology) to implement ICAM activities consistently. However, there was no evidence to ascertain that stakeholders are held accountable for carrying out their roles and responsibilities.</p>

**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
<i>The organization is consistently implementing its ICAM strategy and is on track to meet milestones.</i>
<b>PASS</b> – The Council consistently implemented its ICAM strategy and is on track to meet milestones.
Managed and Measurable
<i>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.</i>
<b>NOT MET</b> – The Council does not have an enterprise architecture like those available in large organizations. The Council’s OSN is not technically a network. OSN is a stand-alone group of laptops connected to a leased wireless access point that provides a leased virtual private network connection to the Trusted Internet Connection portal. The wireless access point is only providing a connection out to the Internet to reach resources hosted elsewhere. The Council has no control over network settings since these are all provisioned on the Internet Service Provider’s side. Each workstation is a stand-alone laptop with a local user account. A user on laptop 1 cannot log into laptop 2 (either locally or over the network) because accounts are only valid to one laptop, and there are no networked resources between the laptops. There are no servers on OSN, and there is no user management tool to manage user accounts. As such, the maturity level was consistently implemented.

## Identity and Access Management

Question 25
<p>To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)</p>
Consistently Implemented
<p><i>The organization consistently implements its policies and procedures for ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.</i></p> <p><b>PASS</b> – 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.</p>
Managed and Measurable
<p><i>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.</i></p> <p><b>NOT MET</b> – 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.</p>

**Identity and Access Management**

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



## Identity and Access Management

### Question 27

To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800- 53 REV. 4: AC-8, PL-4, and PS6)?

#### Consistently Implemented

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

**PASS** - The Council has a unique 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 is directly responsible for implementing all identity, credential, and access management activities. He ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. Additionally, he is the only privileged user, and there is no sensitive information on the network. As such, the Council did not find it necessary to utilize more specific or detailed agreements. Given the small size of the organization and limited complexity of the IT environment, we determined the Council has met the maturity level of consistently implemented for this question.

#### Managed and Measurable

*The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.*

**NOT MET** – Due to the unique structure of the Council’s information systems, the Council did not use automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is not centralized.

**Identity and Access Management**

<b>Questions 28</b>
<p>To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?</p>
<b>Managed and Measurable</b>
<p><i>All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.</i></p> <p><b>PASS</b> – All Council employees, except the CIO, are non-privileged users. The Council implemented strong authentication mechanisms for all non-privileged users and required the use of Personnel Identity Verification (PIV) to gain access to the Council’s government shared service providers.</p>
<b>Optimized</b>
<p><i>The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.</i></p> <p><b>NOT MET</b> - Due to the unique structure of the Council’s information systems, an enterprise-wide single sign on solution that can manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require a financial commitment where the cost-benefits may not be justifiable in the Council’s environment. As such, the maturity level was managed and measurable.</p>

**Identity and Access Management**

<b>Question 29</b>
<p>To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?</p>
<b>Managed and Measurable</b>
<p><i>All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems.</i></p> <p><b>PASS</b> – The CIO is the only privileged user at the Council with assigned moderate-risk designation. He oversees all the IT infrastructure and related activities and is knowledgeable on the Council’s IT environment. As such, the Council’s maturity level is managed and measurable. The CIO also utilizes PIV to gain access to the Council’s system.</p>
<b>Optimized</b>
<p><i>The organization has implemented an enterprise-wide single sign on solution and all of the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.</i></p> <p><b>NOT MET</b> - Due to the unique structure of the Council’s information systems, an enterprise-wide single sign on solution than can manage user (privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis will require a financial commitment where the cost-benefits may not be justifiable in the Council’s environment. As such, the maturity level was managed and measurable.</p>

**Identity and Access Management**

<b>Question 30</b>
<p>To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4)</p>
<b>Consistently Implemented</b>
<p><i>The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed.</i></p> <p><b>PASS</b> – The Council CIO is the lone IT personnel and is directly responsible for implementing all identity, credential, and access management activities. Additionally, he is the only user with privileged access. Given the small size of the organization and limited complexity of the IT environment, we determined the Council has met the maturity level of consistently implemented for this question.</p>
<b>Managed and Measurable</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – The Council did not employ automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.</p>

## Identity and Access Management

### Question 31

To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10

#### Consistently Implemented

*The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.*

**PASS** – There are no remote access connections to the Council’s OSN. Each workstation has help desk software installed, which allows a help desk admin to access the local computer when needed. Such a connection is only created when users request assistance. The help desk employee can only gain access when the user has already logged in to their workstations. The connections use appropriate encryption, and users are automatically logged out after 15 minutes of inactivity.

#### Managed and Measurable

*The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to nonauthorized devices.*

**NOT MET** – The Council is a small organization that did not have the infrastructure, risks, or 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 non-authorized devices.

**Identity and Access Management**

**Question 32**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?*

Questions	Maturity Level
23	Consistently Implemented
24	Consistently Implemented
25	Consistently Implemented
26	Consistently Implemented
27	Consistently Implemented
28	Managed and Measurable
29	Managed and Measurable
30	Consistently Implemented
31	Consistently Implemented
<b>OVERALL</b>	<b>Consistently Implemented</b>

Based on the maturity levels generated from the questions and all testing performed in the Identity and Access Management domain, we concluded that the overall maturity level for the Council’s Identity and Access Management program is **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 for monitoring 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
<p>To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?</p>
<b>Consistently Implemented</b>
<p><i>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).</i></p> <p><b>PASS</b> - According to the Council’s <i>Privacy Program Plan</i>, “None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.” We assessed this maturity level as consistently implemented based on the fact that the Council doesn’t process any form of PII, and the maturity level may not be applicable to the Council’s environment.</p>
<b>Managed and Measurable</b>
<p><i>The organization monitors and analyzes 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.</i></p> <p><b>NOT MET</b> – According to the Council’s <i>Privacy Program Plan</i>, “None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;” therefore the Council did not monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and used that information to make needed adjustments. The organization did not conduct an independent review of its privacy program and make necessary improvements.</p>

**Data Protection and Privacy**

<b>Question 34</b>
<p>To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?</p> <ul style="list-style-type: none"> <li>• Encryption of data at rest</li> <li>• Encryption of data in transit</li> <li>• Limitation of transfer to removable media</li> <li>• Sanitization of digital media prior to disposal or reuse</li> </ul>
<b>Consistently Implemented</b>
<p><i>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.</i></p> <p><b>PASS</b> – According to the Council’s <i>Privacy Program Plan</i>, “None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.” We assessed this maturity level as consistently implemented since the Council does not process any form of PII, and this maturity level should not be applicable to the Council’s environment.</p>
<b>Managed and Measurable</b>
<p><i>The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.</i></p> <p><b>NOT MET</b> – According to the Council’s <i>Privacy Program Plan</i>, “None of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.” Because the Council does not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII information, security controls for protecting PII throughout the data lifecycle are not subject to the monitoring processes and are not applicable.</p>



**Data Protection and Privacy**

Question 35
<p>To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?</p>
<b>Consistently Implemented</b>
<p><i>The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology, audits its DNS records, and ensures the use of valid encryption certificates for its domains.</i></p> <p><b>PASS</b> – The Council consistently monitored inbound and outbound network traffic, ensure that all traffic passed through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the Council checked outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic was quarantined or blocked. The use of email authentication may be unnecessary since the Council doesn’t have a server of its own. In addition, the Council’s website was managed by another agency through an interagency agreement.</p>
<b>Managed and Measurable</b>
<p><i>The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy.</i></p> <p><b>NOT MET</b> – The Council is a small organization that did not have the infrastructure, risks, or resources needed to analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses.</p>

**Data Protection and Privacy**

<b>Question 36</b>
<p>To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?</p>
<b>Consistently Implemented</b>
<p><i>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</i></p>
<p><b>PASS</b> – The Council did not have network servers to store PII. The Council has stand-alone workstations. According to the Council’s <i>Privacy Program Plan</i>, “none of the GCERC Systems create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.” The Council has a Data Breach Response Plan, but the Council does not store PII information. As such, this maturity level is not applicable to the Council’s environment.</p>
<b>Managed and Measurable</b>
<p><i>The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.</i></p>
<p><b>NOT MET</b> – 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 to obtain data supporting metrics accurately, consistently, and in a reproducible format. As such, we determined this maturity level is not applicable to the Council’s environment.</p>

**Data Protection and Privacy**

<b>Question 37</b>
<p>To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5)? (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.)</p>
<b>Consistently Implemented</b>
<p><i>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.</i></p> <p><b>PASS</b> – 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.</p>
<b>Managed and Measurable</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – Based on our inquiry and review of the Council documents, we understand the Council’s OSN does not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII, but the third-party systems the Council uses do. We noted that the Council updates its training program based on statutory, regulatory, mission, program, business process, information systems requirements. Since the Council did not utilize feedback on the content of its training, the Council did not meet this maturity level.</p>

**Data Protection and Privacy**

**Question 38**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?*

Questions	Maturity Level
33	Consistently Implemented
34	Consistently Implemented
35	Consistently Implemented
36	Consistently Implemented
37	Consistently Implemented
<b>OVERALL</b>	<b>Consistently Implemented</b>

Based on the maturity levels generated from the questions and all testing performed in the Data Protection and Privacy domain, we concluded that the overall maturity level for the Council’s Data Protection and Privacy program is **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 Senior Accountable Official for Risk Management. The agency did not process any PII data. PII data needed for human resources and payroll were handled through agreements with a Federal Shared Service Provider whose systems were approved to collect and process PII data. It should be noted 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 *Privacy Program Plan*, “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
<p>To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization-wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800- 53 REV. 4: AT-1; and NIST SP 800-50)</p>
<b>Managed and Measurable</b>
<p><i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.</i></p> <p><b>PASS:</b> The Council has a unique organizational structure with the CIO as the only privileged account user, who is responsible for all day-to-day activities of the Council’s IT security awareness and training program. As a result, we determined resources are allocated in a risk-based manner as the CIO is the lone IT person in the organization.</p>
<b>Optimized</b>
<p><b>Optimized:</b> Per the <i>FY 2019 IG FISMA Metrics</i>, this maturity level is not applicable for this question</p>

**Security Training**

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

## Security Training

Question 41
<p>To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT1).</p>
Managed and Measurable
<p><i>The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.</i></p> <p><b>PASS</b> – The Council monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The Council ensured that data supporting metrics were obtained accurately, consistently, and in a reproducible format. The CIO reviewed all results of testing and made updates to quarterly training based on the analysis as applicable.</p>
Optimized
<p><i>The organization’s security awareness and training activities are integrated across other security-related domains. For instance, common risks and control weaknesses, and other outputs of the agency’s risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program.</i></p> <p><b>NOT MET</b> – The Council did not integrate security awareness and training activities across other security-related domains. For instance, common risks, control weaknesses, and other outputs of the agency’s risk management and continuous monitoring activities did not inform any updates that need to be made to the security awareness and training program.</p>

**Security Training**

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



**Security Training**

<b>Question 43</b>
<p>To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4)</p>
<b>Consistently Implemented</b>
<p><i>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.</i></p> <p><b>PASS</b> – The Council ensured that all systems users completed 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.</p>
<b>Managed and Measurable</b>
<p><i>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.</i></p> <p><b>NOT MET</b> – As a small organization with limited IT infrastructure, the Council does not have much exposure to risk. While the Council conducted phishing awareness training, we did not receive enough evidence to validate that a phishing exercise was performed to measure the effectiveness of the training.</p>

## Security Training

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

**Security Training**

**Question 45**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?*

Questions	Maturity Level
39	Managed and Measurable
40	Managed and Measurable
41	Managed and Measurable
42	Managed and Measurable
43	Consistently Implemented
44	Consistently Implemented
<b>OVERALL</b>	<b>Managed and Measurable</b>

Based on the maturity levels generated from the questions and all testing performed in the Security Training domain, we concluded that the overall maturity level for the Council’s Security Training program is **Managed and Measurable**. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT security training.

**ISCM**

**DETECT FUNCTION AREA**

**Table 8: ISCM**

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

**ISCM**

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

**ISCM**

<b>Question 48</b>
To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE. DP-1; and FY 2019 CIO FISMA Metrics)?
<b>Managed and Measurable</b>
<i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.</i>
<b>PASS</b> – The Council has a small organization structure without a typical network available in a large organization, and the CIO is the lone IT personnel. The Council relied on third-party service providers to manage its information systems. As such, the Council’s service providers are responsible for implementing ISCM activities on those systems. It will be inaccurate to state that the Council does not meet the managed and measurable maturity level.
<b>Optimized</b>
Per the <i>FY 2019 IG FISMA Reporting Metrics</i> , this maturity level is not applicable to this question.

---

**ISCM**

**Question 49**

How mature are 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 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)?

**Optimized**

*The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.*

**PASS** – The Council has a simple and flat organizational structure without formal departments and layers of management. The direct involvement of the CIO and leadership allows the Council to achieve cost-effective IT security objectives and goals that help facilitate the decision-making and minimize cost, risk, and impact on the Council’s mission.

---

**ISCM**

**Question 50**

How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

**Optimized**

*On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.*

**PASS** – On a near real-time basis, the small organizational structure and size enabled the Council to actively adapt its ISCM program to a changing cybersecurity landscape and respond to evolving and sophisticated threats in a timely manner.



**ISCM**

**Question 51**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?*

Questions	Maturity Level
46	Managed and Measurable
47	Managed and Measurable
48	Managed and Measurable
49	Optimized
50	Optimized
<b>OVERALL</b>	<b>Managed and Measurable</b>

Based on the maturity levels generated from the questions and the testing performed in the ISCM domain, we concluded that the overall maturity level of the Council’s ISCM program is **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 facilitate the decision-making and minimize cost, risk, and impact on the Council’s mission.

**Incident Response**

**RESPOND FUNCTION AREA**

**Table 9: Incident Response**

<b>Question 52</b>
<p>To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58.</p>
<b>Consistently Implemented</b>
<p><i>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.</i></p> <p><b>PASS</b> – We inquired of the CIO to determine if the Council experienced any incidents and were informed that no incidents had been reported on the Council’s information system. As such, it will be inaccurate to state that the Council has not met the consistently implemented maturity level as there were no means to verify the implementation of the Council’s policies, procedures, plans, and strategies.</p>
<b>Managed and Measurable</b>
<p><i>The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.</i></p> <p><b>NOT MET</b> – We inquired of the Council CIO whether the Council has experienced any incidents and to determine if the Council monitors or analyzes qualitative and quantitative performance measures on the effectiveness of its incident response system policies, procedures, plans, and strategies. We were informed the Council had not experienced any incidents, as such, we could not determine the Council monitors and analyzes any qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies or validate the Council ensures data supporting metrics were obtained accurately, consistently, and in a reproducible format.</p>

**Incident Response**

<b>Question 53</b>
<p>To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?</p>
<b>Consistently Implemented</b>
<p><i>Individuals are performing the roles and responsibilities that have been defined across the organization.</i></p> <p><b>PASS</b> – We interviewed the Council CIO and inspected the Council documents, and we were able to determine individuals are performing the roles and responsibilities that have been defined across the Council.</p>
<b>Managed and Measurable</b>
<p><i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.</i></p> <p><b>NOT MET</b> – Due to the small organizational structure of the Council and its reliance on third-party service providers that gives the Council limited exposure to the possibility of security incidents, the Council only has part-time incident response team members, serving as more of a virtual incident response team. As such, we could not determine resources are allocated in a risk-based manner for shareholders to implement incident response activities.</p>

## Incident Response

### Question 54

How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS8; and US-CERT Incident Response Guidelines)?

#### Consistently Implemented

*The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.*

**PASS** – The Council is a small organization without a typical network available in a large organization. All Council information systems except the OSN are managed by third-party service providers. As such, the service providers are responsible for implementing processes for incident detection, analysis, and prioritization. In addition, the service providers are responsible for utilizing technologies such as intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.

#### Managed and Measurable

*The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.*

**NOT MET** – The Council is a small organization without a typical network available in a large organization, and the Council relies on third-party service providers to manage its information systems. We were unable to verify the Council’s service providers utilize profiling techniques to measure the characteristics of expected activities on its networks and systems so it can more effectively detect security incidents.

**Incident Response**

<b>Question 55</b>
How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)
<b>Managed and Measurable</b>
<i>The organization manages and measures the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.</i>
<b>PASS</b> – As a small-agency that primarily uses information systems that are hosted by third-party providers, the Council has limited exposure to vulnerabilities and security incidents on its information systems. The Council has not experienced any incidents, and the size of the agency should enable it to respond to any incidents timely.
<b>Optimized</b>
<i>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.</i>
<b>NOT MET</b> – The Council is a small-agency that primarily uses information systems that are hosted by third-party providers. The use of dynamic reconfiguration to stop attacks, misdirect attackers, and to isolate components of systems may be burdensome due to the Council’s organizational structure. As such, the maturity level was managed and measurable.

**Incident Response**

<b>Question 56</b>
<p>To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)?</p>
<b>Consistently Implemented</b>
<p><i>The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner.</i></p> <p><b>PASS</b> – We interviewed the Council CIO, and the Council has a simple flat organizational structure, without formal departments or layers of management like larger organizations. Incident reporting is direct and quick since the Council has a close-knit management team. However, as the Council did not experience any incidents during the evaluation period, we were unable to verify information on incident activities were shared consistently, and security incidents were reported appropriately and in a timely manner.</p>
<b>Managed and Measurable</b>
<p><i>Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.</i></p> <p><b>NOT MET</b> – It should be noted that as the Council is a small organization without the typical IT infrastructures available in a large organization, the agency has limited exposure to incidents and its information systems are managed by third parties. We found no evidence that the Council’s incident response metrics were used to measure and manage the timely reporting of incident information to organization officials and external stakeholders since no incident occurred on the Council system during the period of audit.</p>

**Incident Response**

<b>Question 57</b>
To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800- 86; NIST SP 800-53 REV. 4: IR4; OMB M-18-02; PPD-41)
<b>Managed and Measurable</b>
<i>The organization utilizes Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.</i>
<b>PASS</b> – The Council utilized EINSTEIN 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.
<b>Optimized</b>
Per the <i>FY 2019 IG FISMA Reporting Metrics</i> , this maturity level is not applicable to this question.

## Incident Response

### Question 58

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

- Web application protections, such as web application firewalls.
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies - Information management, such as data loss prevention
- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

#### Managed and Measurable

*The organization uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.*

**PASS** – The Council 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) and did not adjust its incident response processes and security measures accordingly.



**Incident Response**

**Question 59**

*Provide any additional information on the effectiveness (positive or negative) of the organization’s incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?*

Questions	Maturity Level
52	Consistently Implemented
53	Consistently Implemented
54	Consistently Implemented
55	Managed and Measurable
56	Consistently Implemented
57	Managed and Measurable
58	Managed and Measurable
<b>OVERALL</b>	<b>Consistently Implemented</b>

Based on the maturity levels generated from the questions and the testing performed in the Incident Response domain, we concluded that the overall maturity level of the Council’s Incident Response program is **Consistently Implemented**. Since the Council did not own any servers or general support systems and they depend on third-party providers, the Council had limited exposure to the possibility of security incidents and only had part-time incident response team members who serve more as a virtual incident response team. The small organizational structure enables the Council to respond and address security incidents promptly. 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 that 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 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?
Managed and Measurable
<i>Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.</i>
<b>PASS</b> - The Council has 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 is directly responsible for monitoring all IT assets. Further, no IT decisions are made without the CIO’s direct involvement and approval.
Optimized
Per the FY 2019 IG FISMA Reporting Metrics, this maturity level is not applicable to this question.

## Contingency Planning

### Question 61

To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5)

#### 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 has a unique organizational structure and size. However, we noted that the Council had not integrated ICT supply chain concerns into the contingency planning policies and procedures. As such, the maturity level was consistently implemented.

## Contingency Planning

Question 62
To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?
Consistently Implemented
<i>The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA and include characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.</i>
<b>PASS</b> – The Council is a small organization and does not have a typical network available in large organizations that may require an organizational and system-level Business Impact Analysis (BIA). The Council’s information systems are managed by third-party service providers; however, the Council CIO created a BIA for the OSN he manages with the understanding BIA is required.
Managed and Measurable
Per the <i>FY 2019 IG FISMA Reporting Metrics</i> , this maturity level is not applicable to this question.

## Contingency Planning

Question 63
<p>To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800- 53 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?</p>
Consistently Implemented
<p><i>Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.</i></p> <p><b>PASS</b> The Council is a small organization that relies on third-party service providers to manage its information systems, except for the OSN managed by the CIO, and the Council has developed Information Systems Contingency Plan for its OSN. The plan considered activation and notification, recovery, and reconstitution. Each system managed by the service provider receives a FISMA certification ensuring it complied with contingency plans and NIST guidelines are met.</p>
Managed and Measurable
<p><i>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.</i></p> <p><b>NOT MET</b> – The Council did not integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans. The Council owned a 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 those information system contingency plans as the third parties have the responsibility to do so.</p>

## Contingency Planning

Question 64
<p>To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR. IP-10)?</p>
Consistently Implemented
<p><i>Processes for information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.</i></p> <p><b>PASS</b> – 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.</p>
Managed and Measurable
<p><i>The organization employs automated mechanisms to more thoroughly and effectively test system contingency plans. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.</i></p> <p><b>NOT MET</b> – The Council is a small organization that did not have the infrastructure, risks, or resources needed to manage and employ automated mechanisms to more thoroughly and effectively test system contingency plans.</p>

## Contingency Planning

Question 65
<p>To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and National Archives and Records Administration (NARA) guidance on information systems security records)?</p>
Consistently Implemented
<p><i>The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure the potential disruption of the organization’s ability to initiate and sustain operations is minimized and are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information are maintained.</i></p> <p><b>PASS</b> – Though the Council has defined the processes, strategies, and technology for Information System backup and storage, the Council did not have a typical network as found in larger organizations. Given the small size of the organization and limited complexity of the IT environment, the fact that the Council’s Information Systems are managed by third parties, and not subjected to the same physical and cybersecurity risks, we determined the Council has met the maturity level of consistently implemented for this question. In addition, we examined each of the service provider SLA, and determined they addressed contingency planning or continuity of operations.</p>
Managed and Measurable
<p>Per the <i>FY 2019 IG FISMA Reporting Metrics</i>, this maturity level is not applicable to this question.</p>

## Contingency Planning

Question 66
<p>To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR4)?</p>
<b>Consistently Implemented</b>
<p><i>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.</i></p> <p><b>PASS</b> – The Council has a small organizational structure without a typical network available in larger organizations. As a result, the CIO is the lone IT personnel and is directly responsible for monitoring all IT assets. Further, no IT decisions are made without the CIO’s direct involvement and approval. The Council has not experienced any incidents, and there is no evidence of any recovery activities performed.</p>
<b>Managed and Measurable</b>
<p><i>Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders, and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.</i></p> <p><b>NOT MET</b> – The Council has not experienced any incidents, and no recovery activities were performed. As such, we assessed the maturity level as consistently implemented.</p>



## Contingency Planning

### Question 67

*Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?*

Questions	Maturity Level
60	Managed and Measurable
61	Consistently Implemented
62	Consistently Implemented
63	Consistently Implemented
64	Consistently Implemented
65	Consistently Implemented
66	Consistently Implemented
<b>OVERALL</b>	<b>Consistently Implemented</b>

Based on the maturity levels generated from the questions and the testing performed in the Incident Response domain, we concluded that the overall maturity level of the Council's Contingency Planning program is **Consistently Implemented**. The Council had a simple, flat organizational structure without formal departments and layers of management typically found in larger organizations. As a result, the CIO was the lone IT personnel and was directly responsible for monitoring all IT assets. Further, no IT decisions were made without the CIO's direct involvement and approval. The CIO's direct control 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 18, 2019

Richard K. Delmar  
Acting Inspector General  
Department of the Treasury

Re: The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2019

Thank you for the opportunity to review The Gulf Coast Ecosystem Restoration Council Federal Information Security Modernization Act of 2014 Evaluation Report for Fiscal Year 2019. The Council agrees with the report that Council's information security program and practices were effective for the period July 1, 2018 through June 30, 2019. The Council works to ensure that its information assurance program meets the key performance areas for the 5 Cybersecurity Framework security functions that make up the 67 FISMA Reporting Metrics issued by the Department of Homeland Security (DHS).

In fiscal year 2020 the Council will use this evaluation report to inform its information assurance decisions to ensure a continued effective information security program. The Council will also continue its efforts to consistently implement, manage and measure its IT security program at an optimized level in order to support projects and programs to achieve the goals and objectives of the RESTORE Act for restoration in the Gulf Coast region.

Sincerely,

Ben Scaggs  
Executive Director



**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](http://www.treasury.gov/about/organizational-structure/ig)