

**Compliance Audit:
ISO/IEC 27001 ISMS Precertification Audit
Performed by Experis U.S., Inc.**



January 2018

**City Auditor's Office
City of Atlanta**



CITY OF ATLANTA
City Auditor's Office
Amanda Noble, City Auditor
404.330.6452

January 2018

Compliance Audit:

ISO/IEC 27001 ISMS Precertification Audit Performed by Experis U.S., Inc.

Why We Did This Audit

Atlanta Information Management (AIM) requested this audit to assess whether its ISMS (Information Security Management System) is ready to meet certification requirements. ISO/IEC 27001:2013 is the internationally recognized information security management standard. It focuses on establishing and maintaining processes that allow effective and sustainable risk management as threats, risks, and controls change over time.

What We Recommended

We recommend the Chief Information Security Officer work with the Chief Information Officer, Atlanta Information Management, and the body of stakeholders who participate in the Information Security Governance Board to implement our specific recommendations to:

- improve the level of clarity and understanding of the ISMS and its processes
- provide sufficient evidence to demonstrate the effective operation of the ISMS
- establish a documentation portfolio sufficient to meet the ISMS compliance requirements
- establish sufficient degrees of rigor and formality around information security issues management
- establish security metrics that properly track issues, communicate progress and report ISMS performance based on stakeholder needs
- incorporate and maintain an appropriate level of strategic focus in the ISMS
- determine, deploy and maintain and appropriate level of ISMS program resourcing

For more information regarding this report, please use the contact link on our website at www.atlaudit.org.

What We Found

Atlanta Information Management (AIM) and the Office of Information Security have strengthened information security since beginning the ISO 27001 certification project in 2015. Efforts have included monitoring and reporting on vulnerabilities, deploying tools and controls to enhance security, and establishing the Information Security Governance Board, which provides a forum for stakeholder views and participation.

The current Information Security Management System (ISMS), however, has gaps that would prevent it from passing a certification audit, including:

- missing or outdated policies, procedures and guidance documents
- inconsistent definitions of scope
- lack of formal processes to identify, assess, and mitigate risks
- lack of formal processes to manage risks associated with third-party service providers and suppliers
- unclear data classification policies
- incomplete measurement, reporting and communication related to risks

While stakeholders perceive that the city is deploying security controls to protect information assets, many processes are ad hoc or undocumented, at least in part due to lack of resources. Dedicating resources to formalize and document information security management processes would prepare the city for certification, and, more importantly, provide assurance that the city is adequately managing and protecting its information assets.

Management Responses to Audit Recommendations

Summary of Management Responses

Recommendation #1: The CISO should create and deploy a single scope statement that will clarify, document and communicate a common, approved City of Atlanta ISO certification scope to all affected parties.

Response & Proposed Action: Validate Scope with CIO & CISO and recommunicate single scope statement to all stakeholders. **Agree**

Timeframe: FY18 – Q3

Recommendation #2: The CISO should determine and execute corrective actions to close any gaps in the existing policies and/or procedures needed to cover the ISO/IEC 27001/2 domains and clauses included in the Statement of Applicability for assets within the scope of the ISMS.

Response & Proposed Action: Perform gap analysis and validate statement of applicability for the ISMS program. **Agree**

Timeframe: FY18 – Q3

Recommendation #3: The CISO should develop a set of ISMS process flow charts or other procedures that identify the key processes, stakeholders, roles and responsibilities and interested parties involved in the governance and management of the ISMS.

Response & Proposed Action: Define key processes that require flowcharting and procedures for this recommendation and develop the documentation to support this improvement. **Agree**

Timeframe: FY18 – Q4

Recommendation #4: The CISO should develop a set of ISMS operational process flow charts or other procedures that identify the responsibilities of city resources and service providers involved in the deployment and operation of functional controls applicable to the ISMS.

Response & Proposed Action: Define key operational processes that require flowcharting and procedures for this recommendation and develop the documentation to support this improvement. **Agree**

Timeframe: FY18 – Q4

Recommendation #5: The CISO should create a formal process for developing, reviewing and regularly updating the risk assessment, prioritization and risk treatment performed as part of the ISMS.

Response & Proposed Action: Create formal process for ISMS risk management to include but not be limited to annual assessment, prioritization and treatment as approved by our CISO/CISO/Business Decision Makers; require assessment for new systems, annual review of existing systems, and assessment based on changes to production submitted via AIM's change advisory board. **Agree**

Timeframe: FY19

Recommendation #6:	The CISO should create a more visible, comprehensive and timely tracking system for implementation plans, risk treatments and issue remediation activities of assets in the ISMS scope.	
Response & Proposed Action:	Create OIS Action Item Portal to track actions required from ISGB, Internal Audit and vulnerability reports for completions/audit/compliance improvements.	Agree
Timeframe:	FY18 – Q4	
Recommendation #7:	The CISO should create a formal mechanism in the ISMS or department that will track corrective action plans to address audit issues identified for high-risk assets within the ISMS scope and regularly report on progress or deviations to the plans.	
Response & Proposed Action:	Create OIS Action Item Portal to track actions required from ISGB, Internal Audit and vulnerability reports for completions/audit/compliance improvements.	Agree
Timeframe:	FY18 – Q4	
Recommendation #8:	The CISO should establish a consistent ISMS documentation development, review, and approval process that includes identification, tracking and reporting of any open issues related to the ISMS documentation portfolio.	
Response & Proposed Action:	Validate Document management plan to include management of version control of documentation, review and signoff requirements, customer visible versions vs team visibility into all versions. Include use of OIS Action Tracking Portal for ISGB/Audit as key activity and define what's in scope for portal vs. other OIS tools.	Agree
Timeframe:	FY18-Q4	
Recommendation #9:	The CISO should develop a comprehensive inventory of policies, processes, procedures and guidance documents and an action plan to address the gaps in the ISMS and security controls policy portfolio in a timely manner.	
Response & Proposed Action:	Consolidate information into primary ISGB site integrate with OIS team site; replicating date where appropriate.	Agree
Timeframe:	FY18-Q4	
Recommendation #10:	The CISO should develop key policies to address information labeling and handling, and third-party user risk management.	
Response & Proposed Action:	Review information classification policy to be sure language covers audit recommendation. Incorporate into annual policy update to processes and procedures.	Agree
Timeframe:	FY18 Q4	
Recommendation #11:	The CISO should create a list of all previously-identified security issues, vulnerabilities and other process weaknesses that have not been treated to determine the level of effort.	
Response & Proposed Action:	Implementation OIS Action Tracking Portal to include requirements from this recommendation and incorporate into Vulnerability Review Board (VRB).	Agree
Timeframe:	FY18 Q3	

Recommendation #12:	The CISO should create a formal process to document and track the risk rating, prioritization and treatment of all significant identified security issues that add to the level of inherent security risk to the city.	
Response & Proposed Action:	Define, validate and incorporate in to AMPS and make any necessary adjustments to RBBS and APMS as appropriate.	Agree
Timeframe:	FY18 Q4	
Recommendation #13:	The CISO should develop a vulnerability and risk management process that determines when and how data analytics and root cause analysis should be used for the identification and resolution of issues.	
Response & Proposed Action:	Define, validate and incorporate into VRB and make any necessary adjustments to RBBS and APMS as appropriate.	Agree
Timeframe:	FY18 Q3	
Recommendation #14:	The CISO analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate, to provide useful information to each audience.	
Response & Proposed Action:	Define, validate and Incorporate into VRB and make any necessary adjustments to ISMS, as appropriate.	Agree
Timeframe:	FY18 Q2	
Recommendation #15:	The CISO should analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate, to provide useful information to each audience.	
Response & Proposed Action:	Define, validate and Incorporate into ISMS and make any necessary adjustments to other artifacts, as appropriate.	Agree
Timeframe:	FY18 Q4	
Recommendation #16:	The CISO should create a deep-dive analysis process that mandates identifying root causes and remediation actions to eliminate large-scale, chronic issues (e.g., Rapid7 vulnerabilities).	
Response & Proposed Action:	Define, validate and incorporate requirements into VRB and incident management improvements; make any necessary adjustments to RBBS and APMS as appropriate.	Agree
Timeframe:	FY18 Q4	
Recommendation #17:	The CISO should identify and implement key Executive, Management and Operational ISMS Metrics that will be most useful for each stakeholder.	
Response & Proposed Action:	Define, validate and incorporate into ISGB and make any necessary adjustments to other artifacts, as appropriate.	Agree
Timeframe:	FY18 Q2	
Recommendation #18:	The CISO should develop an ISMS Annual Plan that provides a single view of identified strategic initiatives to improve the ISMS and known (or proposed) tactical remediation activities.	
Response & Proposed Action:	Incorporate IS tactical plan as part of the OIS Strategic Plan and ISMS Annual Plan.	Agree
Timeframe:	FY19	

Recommendation #19:	The CISO should create a tracking mechanism that captures and reports on the annual plan initiatives and activities approved by the Information Security Governance Board, as well tracking deviations (positive or negative) from the plan.	
Response & Proposed Action:	Add to tracking portal as action for each year; update annually.	Agree
Timeframe:	FY18 Q4	
Recommendation #20:	The CISO should review the potential need for a separate Tactical ISMS Activities report that provides a status of short- and medium-term activities while the ISMS is still in its developmental stage.	
Response & Proposed Action:	Utilize tactical plan outlined in the Cyber Response Executive Report. Validate ISMS Plan and incorporate IS tactical plan as part of the plan; validate what's required for the activities report since we track action log, strategic plan reviews and project based reviews.	Agree
Timeframe:	FY18 Q4	
Recommendation #21:	The CISO should conduct a comprehensive resource and skills analysis of the Office of Information Security to identify gaps in the appropriate level of security resources required to fully implement and operate the ISMS.	
Response & Proposed Action:	Submit proposed OIS Reorganization request for additional resources.	Agree
Timeframe:	FY18 Q3	
Recommendation #22:	The CISO should conduct a study to determine if additional resourcing is required in the Office of Information Security peer groups and business units to complete the implementation of the ISMS and effectively oversee its operation.	
Response & Proposed Action:	Submit proposed OIS Reorganization request for additional resources.	Agree
Timeframe:	FY18 Q4	
Recommendation #23:	The CISO should create a resourcing plan to allocate appropriate resources to complete the tasks identified in the ISMS project plan and gap remediation plans with a goal of full resourcing in CY2017.	
Response & Proposed Action:	Plan to be proposed in FY18 and implemented by FY19.	Agree
Timeframe:	FY18 Q4	



CITY OF ATLANTA

AMANDA NOBLE
City Auditor
anoble@atlantaga.gov

STEPHANIE JACKSON
Deputy City Auditor
sjackson@atlantaga.gov

CITY AUDITOR'S OFFICE
68 MITCHELL STREET SW, SUITE 12100
ATLANTA, GEORGIA 30303-0312
<http://www.atlaudit.org>
(404) 330-6452
FAX: (404) 658-6077

AUDIT COMMITTEE
Marion Cameron, CPA, Chair
Cheryl Allen, PhD, CPA
Daniel Ebersole

January 16, 2018

Honorable Mayor and Members of the City Council:

We contracted with Experis U.S., Inc. to perform this compliance audit to assess the current state of readiness of the city's ISMS (Information Security Management System) to achieve certification against ISO/IEC 27001:2013, the internationally recognized information security management standard. Atlanta Information Management's Office of Information Security proposed this initiative in 2015 and originally set a target of completing the certification before the end of 2017. Organizations that achieve compliance with the standard benefit from the increased predictability, consistency and effectiveness of the resulting information security processes, which reduce the level of risk to the organization.

The Audit Committee has reviewed this report and is releasing it in accordance with Article 2, Chapter 6 of the City Charter. We appreciate the work completed by Experis U.S., Inc., and the courtesy and cooperation of city staff throughout the audit.

Amanda Noble
City Auditor

Marion Cameron, CPA
Audit Committee Chair

ISO/IEC 27001 ISMS Precertification Audit

Table of Contents

- Introduction 1
- Background..... 1
 - Audit Objectives..... 2
 - Scope and Methodology..... 2
- Findings and Analysis..... 5
 - The ISMS Lacks Some Key Processes Required to Become Certified..... 5
 - The Scope and Processes of the ISMS Are Inconsistently Defined 5
 - ISMS Risk Tracking and Gap Closure Reporting Need Improvement 7
 - Some Key ISMS Documents Are Not Released or Readily Available 9
 - Issues Are Tracked, But Lack Evidence of Root Cause Analysis 10
 - Current ISMS Reporting Is Insufficient to Track and Drive Change..... 12
 - The ISMS Should Focus More on Managing Strategic Risks 14
 - The ISMS Has Chronic Resourcing Challenges..... 15
- Recommendations 17
- Appendices 21
 - Appendix A: Audit Recommendations, Benefits and Proposed Timeframes..... 23
 - Appendix B: Management Review and Response to Audit Recommendations..... 31
 - Appendix C: ISO/IEC 27001/2 Control Objectives and Control Clauses 39

Introduction

We undertook this audit to assess the current state of readiness of the city's ISMS (Information Security Management System) to achieve certification against ISO/IEC 27001:2013, the internationally recognized information security management standard.

Background

Atlanta Information Management's Office of Information Security is responsible for assessing, defining, documenting, deploying and maintaining the information security controls and supporting processes needed to protect sensitive and critical information assets of the city.

To drive the evolution of the information security program within the city, the Chief Information Security Officer proposed an initiative in 2015 to implement a standards-compliant ISMS (Information Security Management System) and pursue certification to ISO/IEC 27001:2013, making Atlanta the first large city in the United States to obtain such a certification.

The initiative originally set a target of completing the ISO Certification Initiative ISMS implementation in 2017 and achievement of the certification before the end of 2017. This audit was undertaken to assess the progress made by the initiative and determine the overall readiness level of the ISMS to achieve certification.

The purpose of pursuing compliance and certification to ISO/IEC 27001:2013 is to establish that the organization has formal, mature and repeatable processes to identify its information assets and establish appropriate operational management of the associated risks. While it may seem that the controls should be at the heart of the certification effort, the standard focuses on establishing and maintaining the security management processes, which are the key to maintaining effective and sustainable risk management as threats, risks and controls change over time.

Organizations that achieve compliance to the standard benefit from the increased predictability, consistency and effectiveness of the resulting information security processes, which reduce the level of risk to the organization. Even if certification is not pursued, organizations like the city often choose to achieve full compliance to gain the benefits that come with a functioning ISMS.

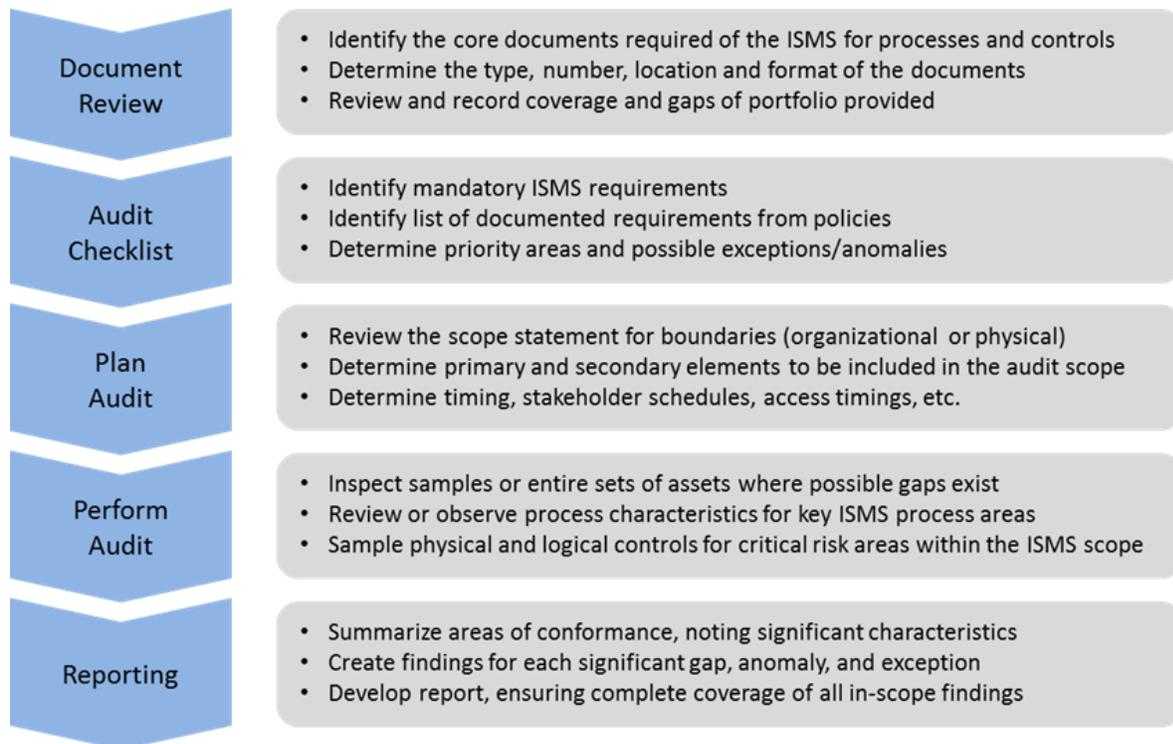
Audit Objectives

This report addresses the following objectives:

- Assess whether the city’s information security policies and procedures conform to the requirements of ISO/IEC 27001:2013
 - Assess whether the city’s Office of Information Security has effectively implemented the policies and procedures
 - Make recommendations to assist the Office of Information Security to achieve ISO/IEC 27001:2013 certification
-

Scope and Methodology

This audit was conducted in accordance with information security management system auditing practices. The scope of the audit included an evaluation of the information security services, processes, and controls described in the ISMS documentation to protect the confidentiality, integrity and availability of the city’s critical information assets within the scope of the ISMS. A list of twenty information assets was provided at the outset of the audit as the inventory to be considered within the scope of the ISMS. Our audit utilized the Experis ISMS Audit Methodology, which included the following tasks and activities.



Early in the audit execution it was discovered there were some significant documentation deficiencies related to both the ISMS processes and the functional controls, which required the methodology to be adjusted to evaluate the level of coverage provided by the current ISMS processes, in addition to ascertaining the compliance gaps of the deployed ISMS against the requirements of the standard.

Findings and Analysis

The ISMS Lacks Some Key Processes Required to Become Certified

Atlanta Information Management and the Office of Information Security have made substantial progress since the ISO 27001 Certification Project began in 2015, including the establishment of the Information Security Governance Board, which provides a forum for stakeholder views and participation. The current ISMS, however, has gaps in a significant number of the required information security management processes that would prevent it from passing a certification audit. These gaps include missing or outdated policies, procedures and guidance documents; inconsistent definitions of scope, control applicability, and risk treatment; and incomplete measurement, reporting and communication related to risks to sensitive and critical information assets.

In addition to the certification gaps, we identified several issues with the original project scope that appear to have been due to a misunderstanding of the requirements of the ISO/IEC 27001:2013 standard, but which led the project team to eliminate some critical documentation from the project plan.

While stakeholders perceive that the city is deploying security controls to protect information assets, the current state of the ISMS lacks many forms of evidence that management and auditors need to confirm the adequacy of the protective measures deployed and to identify issues requiring attention. These gaps in processes and reporting could allow security issues to go undetected or untreated for periods of time that would pose an increased inherent risk level to the city that a properly functioning ISMS would address.

We recommend the chief information security officer work with the chief information officer, Atlanta Information Management, and the body of stakeholders that participate in the Information Security Governance Board to continue to: 1) implement the existing ISMS project plan; and, 2) establish action plans to address each of the recommended actions identified in this audit report. These recommendations range from eliminating gaps in the current state policies and procedures, to clarification of the ISMS scope, to improvements in the ISMS measurement and reporting, to dealing with a perceived chronic resource challenge that impacts the ISMS implementation as well as its ongoing operation.

The Scope and Processes of the ISMS Are Inconsistently Defined

The ISMS documentation portfolio contains a substantial number of documents, many of which were created or revised within the past 12-18 months, but our overall assessment is the ISMS has a number of documentation gaps that impact the ability of the stakeholders to understand key aspects of the included scope and expected delivery elements of the ISMS. There are consistency issues, such as the three different definitions of the ISMS scope, and spotty coverage of the control domains, as evidenced by the provided security policy portfolio covering some, but not all of the required control objectives of ISO/IEC 27001:2013 and ISO/IEC 27002:2013. The absence of some policies was attributed to what appeared to be a

misunderstanding of what documents were mandatory for an ISMS during the early project planning efforts. This led to a number of key objectives and clauses of both standards being classified as optional, and therefore not being included in the ISMS project plan.

The scope has at least three conflicting definitions. We identified three formal documents that define the scope of the ISMS (ISMS-4.3, A.8.1.1, ISMS Program Structure), each in a different way, which has led to confusion among the stakeholders about what services, critical systems, locations, and control domains are included in the deployed ISMS. Although the scope of a certified ISMS can be adjusted over time, it is critical that there be a consistent definition and understanding of the scope of the ISMS to establish a common view of what the ISMS is meant to achieve. The inconsistencies also validate there are underlying issues with how ISMS documents are developed, reviewed and released.

1. *We recommend the Chief Information Security Officer and Information Security Governance Board create and deploy a single scope statement that will clarify, document and communicate a common, approved ISMS certification scope to all affected parties.*

Existing policies provide high-level direction, but lack supporting processes. The policies consistently provided high-level guidance of the responsibilities associated with the specific security domain, but the majority had no formal documentation that would constitute supporting guidance in the form of process or procedure documentation to assist with the implementation or evaluation of the controls. The stakeholders interviewed consistently indicated that the city relies on the inherent skills of the people assigned to support systems to know how to execute their duties, what controls to deploy, and which configurations are appropriate for each type of system, network or application involved. This reliance on institutional knowledge with little to no documentation presents a potentially significant risk to the city, particularly if business discontinuities or security incidents occur and key staff are not available to respond.

2. *We recommend the Chief Information Security Officer and Information Security Governance Board determine and execute corrective actions to close any gaps in the existing policies and/or procedures needed to cover the ISO/IEC 27001/2 clauses included in the Statement of Applicability for the assets within the scope of the ISMS.*

Some ISMS domains and control objectives do not have formal policies or procedures. Some of the key management and governance processes expected to be included in a certified ISMS rely on the Information Security Governance Board activities and do not have formal policy or procedure documents. Of the seven control domains in ISO/IEC 27001, this gap includes most of the clauses of control domains 7, 8, 9, and 10, which define the core elements of the ISMS that provide the support, operation, performance evaluation and improvement process capabilities of the ISMS. While the Information Security Governance Board has embraced its role in governance and has shown a dedication to its role in managing the information security risks to critical assets, the lack of formal documentation and governance reporting makes it difficult to determine the overall effectiveness of the ISMS or

have assurance the ISMS has the capabilities to identify and address issues in a timely manner, which raises the level of inherent risk to the city.

- 3. We recommend the Chief Information Security Officer and Information Security Governance Board develop a set of ISMS process flow charts or other procedures that identify the key processes, stakeholders, roles and responsibilities and interested parties involved in the governance and management of the ISMS.*

Some Annex A domains and control objectives do not have formal policies or procedures.

A significant number of the controls identified as applicable for risk treatment of the information assets within the scope of the ISMS do not have formal policy or procedure documents. Of the 14 control domains, 35 control objectives and 114 controls specified in ISO/IEC 27002, only about one-third are covered by current policy documents, and only a small number of those were included in any formal or informal process documentation provided during the discovery task of the audit. Key control areas, such as access control, system acquisition, development and maintenance, communications security and supplier relationships are often among the most critical control areas needed to provide effective risk treatment and protect information assets, yet these areas have few policies or other guidance documents identified in the formal ISMS policy portfolio. This is believed to be one of the findings related to the misunderstanding of the controls made at the outset of the ISO Certification Initiative that incorrectly excluded a number of controls needed for the ISMS to become certified.

- 4. We recommend the Chief Information Security Officer develop a set of ISMS operational process flow charts or other procedures that identify the responsibilities of city resources and service providers involved in the deployment and operation of functional controls applicable to the ISMS.*

ISMS Risk Tracking and Gap Closure Reporting Need Improvement

The processes associated with risk identification, risk assessment, and risk treatment, and the documentation that should provide tracking of the risk treatment deployments do not have the formality and rigor needed to demonstrate effective risk management. Some of the gaps may be due to the ISMS not being fully deployed and operational in all aspects, but this is a critical area of governance that is required to support many other aspects of the ISMS operation, including certification.

Risk assessment of critical assets does not have adequate tracking data. The documentation provided included the output of risk assessments performed for the portfolio of twenty critical systems in 2016, with numerous updates in the change history, but there is insufficient data to determine what information in the document was updated at each point in time. In addition, the latest version of the document indicates some assets were supposed to go through re-assessment by a date that is before the latest update of the risk assessment document. As the risk assessment is one of the most critical documents underpinning the effective operation of the ISMS, it is required to be complete, accurate, and maintained to

clearly communicate the risks that must be addressed by the other ISMS processes and control deployments to eliminate unacceptable risks to the city.

- 5. We recommend the Chief Information Security Officer create a formal process for developing, reviewing and regularly updating the risk assessment, prioritization and risk treatment performed as part of the ISMS.*

Implementation plans and tracking of risk treatments are not evident. We reviewed many documents that conveyed information about the inherent risk profiles, risk treatments and residual risks of the twenty critical assets within the scope of the ISMS, but identified numerous instances where the information provided appeared to be out-of-date or incomplete, including instances where the risk treatment was planned to be completed weeks before the date of the latest version of the tracking document. Based on the available information, it was not possible to determine if agreed risk treatments were ever implemented, or if so, when they were implemented. The risk treatments also identified what appeared to be a subset of the total controls defined as applicable in the ISMS Statement of Applicability, which makes it difficult to determine the actual control set that is deployed for each critical asset at any point in time without inspecting the system. This indeterminate state of control deployment could obscure significant risks in the operational environment and would constitute a major non-compliance if not corrected prior to a certification audit.

- 6. We recommend the Chief Information Security Officer create a more visible, comprehensive, and timely tracking system for implementation plans, risk treatments, and issue remediation activities of assets in the ISMS scope.*

Tracking of mitigation plans for high-risk audit issues is lacking. We identified several high-risk audit findings from past application and system audits that we could not locate corrective action plans or issue closure reporting for. In one case, several issues related to segregation of duties on the existing Oracle HR system had corrective action plans that indicated the issues would be closed as part of the Oracle platform migration currently underway. The documentation provided did not provide evidence that the issues had been formally included in the project requirements and the Information Security Governance Board did not have any tracking mechanism that identified who was responsible for ensuring these requirements were part of the final design, or validating the audit issues were closed as part of the production release review. Identifying issues and determining corrective actions must be accompanied by a tracking system that can track and report progress or deviation from the agreed action plans to avoid critical issues from exposing the city to unnecessary risks for longer than is necessary. This issue would also be a possible major non-conformance if not corrected prior to a certification audit.

- 7. We recommend the Chief Information Security Officer work with the City Auditor's Office to create a formal mechanism (in the ISMS or other department) that will track corrective action plans to address audit issues identified for high-risk assets within the ISMS scope and regularly report on progress or deviations to the plans.*

Some Key ISMS Documents Are Not Released or Readily Available

Many documents we reviewed had a consistent look-and-feel, recent revision and formal approval, but other policies and supporting documents had variations in format and consistency, and many lacked formal approval. Other key ISMS and control documents that we requested were not provided, and interviews indicated they were not included in the released policy portfolio as they were believed to be optional. This is another area where the misunderstanding in the early planning stages of the ISMS has led to the portfolio not including all documents needed to achieve certification. In addition, it would typically be expected that an operational ISMS would have supporting procedures or other operational guidance documents for the core ISMS governance and management processes at a minimum to demonstrate a means to provide a consistent execution of security management.

ISMS documentation approval and management process is inconsistently followed. We were unable to identify a formal policy or procedure for documentation approval and management in the formal ISMS policy repository, but did locate a draft document in a broad archive of uncontrolled and draft documents provided later in the audit. This procedure is a critical element in a properly functioning ISMS as it establishes a set of required activities and approval flow that must be used to keep ISMS documentation consistent, complete and aligned with the latest management decisions regarding risk assessment and acceptance. In one case, we discovered a policy (ISMS-5.3) that was revised in early 2017 that named the Chief Information Officer as the approver of all ISMS policies, yet policies were approved after that date by the Chief Information Security Officer, indicating either an error in the assignment of responsibilities or a consistency issue with policy compliance, either of which could affect the ability of the city to pass a certification audit.

8. *We recommend the Chief Information Security Officer establish a consistent ISMS documentation development, review, and approval process that includes identification, tracking and reporting of any open issues related to the ISMS documentation portfolio.*

Information labeling and handling requirements are not defined or communicated. We determined there was an information classification policy (ISMS-A.8.2.1 and A.8.2.3) which established a tiered data classification system and provided minimal guidance on the risks and impacts of improper classification, but the policy did not provide guidance on the appropriate (or preferred) ways to label and handle sensitive information, nor did it reference a labeling and handling standard or other guidance document that established the acceptable practices. The policy also indicated that printed information marked “Internal Use Only” could only be released to the owning department or an authorized courier, which would essentially preclude providing printed copies of policies to contractors, vendors and other authorized third parties and seriously impact the ability of the city to enforce policy provisions on users who are not city employees. As the information classification policy and the supporting labeling and handling practices are core behaviors in establishing and maintaining adequate information protection, the lack of guidance in this area could result in significant levels of preventable risks to the city and its information assets over time. This might also be considered as a non-conformance if not corrected prior to a certification audit.

9. *We recommend the Chief Information Security Officer develop a comprehensive inventory of policies, processes, procedures and guidance documents and an action plan to address the gaps in the ISMS and security controls policy portfolio in a timely manner.*

No third-party risk management process exists (including awareness and on-boarding). The provided ISMS policy portfolio did not contain any specific policies or other guidance related to managing the risks associated with third-party service providers and supplier relationships, as defined in ISO/IEC 27002:2013 Domain 15. We also discovered that the current mechanisms for tracking and managing human resources only includes employees of the city and does not include provisions to specifically address the communication of information protection responsibilities and risk management of third parties entrusted to access, operate or process information created, owned or in the care of the city. Due to the extensive use of third-parties and other external service providers to support the various missions of city departments, including some of the critical assets in the scope of the ISMS, this poses a significant area of exposure that should have been included in the scoping, risk assessment, risk treatment and control deployment of the initial ISMS. Unless the scope of the ISMS includes only assets and services that are managed exclusively by internal city employees, the risks posed by a lack of direct protective measures for supplier relationships could have a negative impact on the city and might impact the ability of the city to achieve ISO certification.

10. *We recommend the Chief Information Security Officer develop key policies to address information labeling and handling, and third-party user risk management.*

Issues Are Tracked, But Lack Evidence of Root Cause Analysis

Atlanta Information Management and the Office of Information Security regularly publish metrics and reports to a number of audiences, but some of the metrics did not appear to have associated analysis to determine the root causes of the issues and lacked any reporting of corrective actions or target dates to reduce the risks posed by the issues. In one case, monthly vulnerability scan results indicated the presence of 1,500-2,000 severe vulnerabilities in the scanned population, with a history that went back over a year with no evidence of mitigation of the underlying issues. Another example is the presence of almost 100 servers running versions of Windows 2003 Server software, which was declared obsolete and passed end-of-life almost two years ago. Even though these servers support key departments throughout the city, there did not appear to be an action plan to migrate their services to newer platforms, or add compensating controls to reduce the risks posed by these systems while a migration plan could be determined. Identification and treatment of critical and severe security issues is a core capability expected of an operating ISMS, and is a key element in the ISMS delivering effective security and risk management.

Current IT/IS resources are not sufficient to handle discovered weaknesses. In the example noted, it was stated during multiple interviews that the departments tasked with dealing with the thousands of vulnerabilities discovered by the monthly scans do not have enough time or

tools to properly analyze and treat the systems. While no formal reports or other evidence was provided to substantiate this assertion, this level of backlog is typical of organizations without a mature vulnerability management program and tools to support the quick and efficient handling of issues.

- 11. We recommend the Chief Information Security Officer create a list of all previously-identified security issues, vulnerabilities and other process weaknesses that have not been treated to determine the level of effort and action plans required to eliminate, mitigate, transfer or accept the risks.*

Unaddressed issues have resulted in increased inherent risk. The large number of severe and critical vulnerabilities identified by the monthly vulnerability scan results metric has existed for so long the organizations responsible for this area have essentially become complacent and no longer take action other than to update the monthly report. The significance of such a backlog of severe and critical vulnerabilities without corrective actions is evidence of procedural, technical or administrative failures in the risk management and security management processes. This situation represents a significant level of preventable risk exposure to the city and is also a deviation from the expected functionality provided by an ISMS, which could be interpreted as a major non-conformance if not addressed prior to a certification audit.

- 12. We recommend the Chief Information Security Officer create a formal process to document and track the risk rating, prioritization and treatment of all identified critical and severe security issues.*

Data analytics and root cause analysis could help reduce vulnerabilities. We saw no evidence of a process, tools, or other means Atlanta Information Management or Office of Information Security use to analyze the significant volume of vulnerabilities to identify root causes that could be addressed to eliminate some contributing factors and potentially reduce the recurrence of issues. Use of data analytics has become a common practice in organizations that have mature security management and vulnerability management programs. Data analytics provide the ability to identify common issues and discern patterns in anomalies that might be dealt with using a common treatment plan. Simple tools, such as table-driven configuration reviews and patch management analysis techniques, might also reveal corrective actions that could be implemented during periodic maintenance windows. The absence of consistent analyses techniques indicates that current operational processes are insufficient to address the level of monthly vulnerabilities, which poses a significant latent risk to the city.

- 13. We recommend the Chief Information Security Officer develop a vulnerability and risk management process that determines when and how data analytics and root cause analysis should be used for the identification and resolution of issues.*

Current ISMS Reporting Is Insufficient to Track and Drive Change

The documentation provided during the audit revealed metrics used to report discrete measurements of security attributes, but the documents did not include metrics that would constitute regular assessment and reporting of the operational status of the ISMS or the level of inherent or residual information risk to city information assets. The focus of the metrics seemed to be more on reporting easily-identified values rather than focusing on identification of the issues and reporting on mitigation efforts. Examples included: 1) reporting of the number of blocked malware “calling home” addresses instead of reporting the Mean-Time-To-Detect (MTTD) or Mean-Time-To-Repair (MTTR) for malware-infected systems and action plans to reduce the MTTD and MTTR; 2) Reporting the monthly # of Phishing SPAM emails instead of a monthly rolling average of the percentage of users that passed a phishing test and action plans to change the filtering and user awareness to decrease the susceptibility to phishing; and, 3) reporting the number of Critical, Severe, and Moderate vulnerabilities discovered during monthly scans instead of the MTTR for vulnerabilities in each category or the percentage of vulnerabilities closed within 1, 7, or 30 days of discovery and an action plan to drive down the exposure window of vulnerabilities for critical systems.

We also observed the metrics and reports seemed to provide information that would be useful to operational personnel, but would not assist management in adjusting priorities or executives in making better informed decisions. While operational metrics and measures are a vital part of delivering effective information security and risk management, not including specific metrics to address the motivations and needs of other key audience types is a missed opportunity to demonstrate the value of the ISMS and communicate the rationale for resourcing and funding. In particular, resource utilization and workload metrics can provide decision support information and value to all three audience types if properly designed and executed.

We noticed the issues with the ISMS metrics are not unique to the Office of Information Security organization; other measures and metrics included in the documentation and observed during the discovery interviews revealed a general tendency to publish technical metrics that provide discrete data, but rarely provide analysis, targets, process limits or other information that would help managers and operations staff make better decisions. The potential value of a metric is lost when it does not include information that ties the reported results to an organizational mission statement, strategic improvement, or operational goal.

Current metrics report technical details but do not show intended outcome or risk level. We observed the metrics and reports seemed to provide information that would be useful to operational personnel, but would not assist management audiences in adjusting priorities or executive audiences in making better informed decisions. The metrics currently reported at the Information Security Governance Board and provided to other stakeholders provide graphs of monthly measurements, such as the number of vulnerabilities of a certain risk level, but do not include an indication of the target level to be achieved or a goal for acceptable risk level. The lack of any goals or other indications of expected outcome or change significantly reduces the value that can be derived from the information, particularly for non-technical audiences.

- 14. We recommend the Chief Information Security Officer analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate to provide useful information to each audience.*

No metrics report the status or direction of the ISMS. None of the metrics provided seem intended to report on the performance or direction of the ISMS or the assessment and acceptance of risk managed by the Information Security Governance Board. Such measures could demonstrate the value of the ISMS and communicate the rationale for resourcing and funding. Resource utilization and workload metrics can provide decision support information and value to all three audience types if properly designed and executed. Nascent ISMS initiatives often include reporting of progress against their implementation plans and deviations in resources or project milestones, while mature ISMS implementations often include routine reporting of issues, asset risks, changes in threats, and operational performance. Some form of measurement and reporting related to the ISMS performance is an expected element that needs to be addressed prior to a certification audit.

- 15. We recommend the Chief Information Security Officer identify and create ISMS Program Metrics that measure and report key success criteria and progress against the goals of the ISMS.*

No data analysis process is linked to the current metrics and reporting. Some of the examples we observed (e.g., monthly vulnerabilities) describe latent risk conditions that have persisted for a long time without indication of corrective action or compensating controls. There was no evidence provided that indicated the level of risk posed by the severe and critical vulnerabilities had been accepted by the business owners or the Information Security Governance Board, nor was there any evidence provided that showed this large-scale issue had been analyzed and broken down into manageable issues based on the root cause or other criteria. Other metrics also appeared to lack analysis that might help determine the approach or direction for eliminating, remediating, transferring, or accepting the residual risk. Establishing a formal analysis process that can be used for significant or persistent issues would be consistent with the principles of risk management that should be incorporated into the ISMS and would provide useful information for the annual ISMS program review and continuous improvement activities.

- 16. We recommend the Chief Information Security Officer create a deep-dive analysis process that mandates identifying root causes and remediation actions to eliminate large-scale, chronic issues (e.g., Rapid7 vulnerabilities).*

Stakeholder metric requirements should be identified and delivered by audience type. Metrics published to all stakeholder audience types (e.g., Executive, Management, Operational) focused almost exclusively on discrete technical measures related to the operational environment without consideration of the information based on stakeholder needs. We believe this had the result of providing information that was not suited to many audience members and might have conditioned the stakeholders to become complacent about the underlying risks present in city information systems. There was also no evidence that

information security metrics were discussed regularly to determine their usefulness or identify improvements based on the intended audience member needs. The development of additional metrics, differentiated by stakeholder types would provide an opportunity to focus communications more precisely on information that would help groups of stakeholders more fully understand the current state of risk in their environment, and enhance their ability to make decisions regarding prioritization or allocation of resources.

17. We recommend the Chief Information Security Officer identify and implement key Executive, Management and Operational ISMS Metrics that will be most useful for each stakeholder.

The ISMS Should Focus More on Managing Strategic Risks

The documentation provided during the audit and the stakeholder interviews revealed the ISMS focuses primarily on managing and addressing known issues based on the perceived operational priorities, which results in a significant amount of its efforts being directed on tactical issues rather than a balanced focus on both tactical and strategic goals. One of the results of this tactical focus is too little attention paid to achieving strategic risk reduction goals or identifying and resolving chronic control issues. The ISMS should be the primary focal point for identifying, developing, and addressing strategic information security and information risk management goals, and the processes and activities it deploys should support those goals.

Current ISMS processes are primarily tactical and reactive. Many of the current ISMS and security-related risk mitigation activities appear to be tactical or reactive in nature, with little regard for the impact of resource redirection on other strategic or organizational initiatives. As the ISMS, through the Information Security Governance Board, is the focal point for strategic information security management, it should have a formal process and accompanying documentation that captures, communicates, and tracks the strategic initiatives and associated action plans to all stakeholders. These strategic plans should provide the direction needed for other organizations and peer groups, such as Atlanta Information Management, to execute their management and operational roles in a manner that fully supports the security goals and required security compliance levels without the need for excessive oversight or involvement of the ISMS or Information Security Governance Board. Organizations often use some form of an annual plan that outlines the primary goals of the ISMS to demonstrate their commitment to regular review and continuous improvement of the ISMS. Such a document often sought as part of a certification audit.

18. We recommend the Chief Information Security Officer develop an ISMS Annual Plan that provides a single view of identified strategic initiatives to improve the ISMS and known (or proposed) tactical remediation activities.

ISMS success will require strategic risk management and tracking. Documents provided did not include an annual plan for the ISMS and there did not appear to be any process or mechanism to identify and regularly track and report on progress on ISMS activities. The project plan for the overall ISO Certification Initiative seemed to only be updated

occasionally, which prevented it from being used as an indicator of progress or an outlook for resourcing over any upcoming period. There was no ISMS process that provided a composite view of all projects and initiatives related to security, and routinely reported on progress and exceptions to keep management informed and assist with resource allocations or program adjustments.

19. *We recommend the Chief Information Security Officer create a tracking mechanism that captures and reports on the annual plan initiatives and activities approved by the Information Security Governance Board, as well tracking deviations (positive or negative) from the plan.*

Some bias toward short-term remediation efforts is expected in early stages. Discussion with stakeholders during the audit indicated that stakeholders are committed to the overall ISMS goals, and the need to better manage the information risks facing the city. But, when asked about the current state of risk management represented by the monthly metrics, they also agreed that not enough was being done to deal with the identified risks and exposures. Stakeholders agreed that most of the ISMS activities fall on only a couple of resources, which did not seem sufficient to accomplish all of the important activities in the time available. It was apparent that the ISMS should consider adopting some form of tailored tracking and reporting mechanism to identify the short-term (tactical) activities that need to be completed in order to be fully prepared for certification and provide greater visibility of any resource or timing issues that might impede completion within 2017. The actions recommended by this audit will also need to be included in whatever mechanism is chosen to track the tactical activities.

20. *We recommend the Chief Information Security Officer review the potential need for a separate Tactical ISMS Activities report that provides a status of short- and medium-term activities while the ISMS is still in its developmental stage.*

The ISMS Has Chronic Resourcing Challenges

The evidence obtained through documentation review and stakeholder interviews revealed an environment where resources often appear to be inadequate to deliver all of the assigned responsibilities. This was evident in our review of the project plan and outcome of the ISO Certification Project, which would have required a notional staffing level of approximately two full-time equivalent resources over the two-year projected implementation timeframe, but the project seems to have had far less than one full-time equivalent resource for most of the execution timeframe. This chronic shortage of resources appears to have had some impact on the consistency and completeness of the documentation, metrics and reporting associated with the ISMS as many of these tasks seem to have been completed on a time-available basis rather than according to the project execution plan. During stakeholder interviews, it became apparent that other departments participating in the ISMS initiative have similar resource limitations. A concern is that there was no evidence of the resource shortage being tracked and reported, nor any documentation that described the project or activity delays, or management's acceptance of the risk. The absence of this evidence indicates management may not be fully aware of the potential impacts and organizational

risks likely to result from the resource limitation or the project prioritization and/or deferments that are occurring within the ISMS and other departments.

The ISMS staffing level is less than needed to finish the effort in the planned timeframe. As previously described, the audit revealed there was a misunderstanding at the outset of the ISO Certification Initiative that resulted in the improper classification of many policies and procedures required to achieve certification as optional. In addition, our analysis of the project execution thus far indicates the resourcing of the project has not been sufficient to complete all the activities needed to define the ISMS, such as the incomplete and inconsistent documentation portfolio.

21. We recommend the Chief Information Security Officer conduct a comprehensive resource and skills analysis of the Office of Information Security to identify gaps in the appropriate level of security resources required to fully implement and operate the ISMS.

Security support and peer group staffing are also insufficient for defined tasks. Other peer groups within Atlanta Information Management that would be expected to support the Office of Information Security in the execution of the ISMS also appear to have chronic resource shortages that impact their ability to stay ahead of the security issues, such as migration of obsolete operating systems, patch management, and vulnerability management. The presence of persistent or chronic security issues and lack of timely closure can be seen as a failure of the ISMS and deemed to be a non-conformance that could impact certification if not addressed prior to a certification audit.

22. We recommend the Chief Information Security Officer conduct a study to determine if additional resourcing is required in the Office of Information Security peer groups and business units to complete the implementation of the ISMS and effectively oversee its operation.

Additional resources are needed to become certification-capable by end of 2017. Our analysis indicates that the additional activities identified by the recommendations associated with this audit will exacerbate the resource shortage. Our analysis also indicates the Office of Information Security team is not sufficiently staffed to perform the activities required to operate the ISMS and address security risk management issues, such as vulnerability management, exception processing and incident management without some additional resources or assistance from Atlanta Information Management. A chronic resource shortage for the ISMS will likely impact the ability of the city to achieve ISO certification.

23. We recommend the Chief Information Security Officer create a resourcing plan to allocate appropriate resources to complete the tasks identified in the ISMS project plan and gap remediation plans with a goal of full resourcing in 2017.

Recommendations

To improve the level of clarity and understanding of the ISMS and its processes, the CISO Chief Information Security Officer (CISO) should:

1. Create and deploy a single scope statement that will clarify, document and communicate a common, approved City of Atlanta ISO certification scope to all affected parties.
2. Determine and execute corrective actions to close any gaps in the existing policies and/or procedures needed to cover the ISO/IEC 27001/2 domains and clauses included in the Statement of Applicability for assets within the scope of the ISMS.
3. Develop a set of ISMS process flow charts or other procedures that identify the key processes, stakeholders, roles and responsibilities and interested parties involved in the governance and management of the ISMS.
4. Develop a set of ISMS operational process flow charts or other procedures that identify the responsibilities of city resources and service providers involved in the deployment and operation of functional controls applicable to the ISMS.

To provide sufficient evidence to demonstrate the effective operation of the ISMS, the Chief Information Security Officer should:

5. Create a formal process for developing, reviewing and regularly updating the risk assessment, prioritization and risk treatment performed as part of the ISMS.
6. Create a more visible, comprehensive and timely tracking system for implementation plans, risk treatments and issue remediation activities of assets in the ISMS scope.
7. Create a formal mechanism in the ISMS or department that will track corrective action plans to address audit issues identified for high-risk assets within the ISMS scope and regularly report on progress or deviations to the plans.

To establish a Documentation Portfolio sufficient to meet the ISMS compliance requirements, the Chief Information Security Officer should:

8. Establish a consistent ISMS documentation development, review, and approval process that includes identification, tracking and reporting of any open issues related to the ISMS documentation portfolio.
9. Develop a comprehensive inventory of policies, processes, procedures and guidance documents and an action plan to address the gaps in the ISMS and security controls policy portfolio in a timely manner.
10. Develop key policies to address information labeling and handling, and third-party user risk management.

To establish sufficient degrees of rigor and formality around information security Issues Management, the Chief Information Security Officer should:

11. Create a list of all previously-identified security issues, vulnerabilities and other process weaknesses that have not been treated to determine the level of effort and action plans required to eliminate, mitigate, transfer or accept the risks.
12. Create a formal process to document and track the risk rating, prioritization and treatment of all significant identified security issues that add to the level of inherent security risk to the city.
13. Develop a vulnerability and risk management process that determines when and how data analytics and root cause analysis should be used for the identification and resolution of issues.

To establish Security Metrics that properly track issues, communicate progress and report ISMS performance based on stakeholder needs, the Chief Information Security Officer should:

14. Analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate, to provide useful information to each audience.
15. Analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate, to provide useful information to each audience.
16. Create a deep-dive analysis process that mandates identifying root causes and remediation actions to eliminate large-scale, chronic issues (e.g., Rapid7 vulnerabilities).
17. Identify and implement key Executive, Management and Operational ISMS Metrics that will be most useful for each stakeholder.

To incorporate and maintain an appropriate level of Strategic Focus in the ISMS, the Chief Information Security Officer should:

18. Develop an ISMS Annual Plan that provides a single view of identified strategic initiatives to improve the ISMS and known (or proposed) tactical remediation activities.
19. Create a tracking mechanism that captures and reports on the annual plan initiatives and activities approved by the Information Security Governance Board, as well tracking deviations (positive or negative) from the plan.
20. Review the potential need for a separate Tactical ISMS Activities report that provides a status of short- and medium-term activities while the ISMS is still in its developmental stage.

To determine, deploy and maintain an appropriate level of ISMS Program Resourcing, the Chief Information Security Officer should:

21. Conduct a comprehensive resource and skills analysis of the Office of Information Security to identify gaps in the appropriate level of security resources required to fully implement and operate the ISMS.
22. Conduct a study to determine if additional resourcing is required in the Office of Information Security peer groups and business units to complete the implementation of the ISMS and effectively oversee its operation.
23. Create a resourcing plan to allocate appropriate resources to complete the tasks identified in the ISMS project plan and gap remediation plans with a goal of full resourcing in CY2017.

Appendices

Appendix A: Audit Recommendations, Benefits and Proposed Timeframes

ISMS Clarity (IC): The scope and processes of the ISMS are inconsistently defined.			
#	Recommended Activity and Short Description	Expected Benefits	Time Frame
IC1	The Chief Information Security Officer should create and deploy a single scope statement that will clarify, document and communicate a common, approved ISMS certification scope to all affected parties.	- Creating and communicating an agreed scope will demonstrate the overall ISMS program and all affected parties are working on a common set of goals and objectives, which is critical to certification.	Short-term
IC2	The Chief Information Security Officer should determine and execute corrective actions to close any gaps in the existing policies and/or procedures needed to cover the ISO/IEC 27001/2 domains and clauses included in the Statement of Applicability for assets within the scope of the ISMS.	- Creating a comprehensive set of ISMS documents that include processes or other guidance for implementing the policy provisions will create a strong foundation for identifying, treating and managing information security risks and demonstrating the capabilities needed for certification.	Mid-term
IC3	The Chief Information Security Officer should develop a set of ISMS process flow charts or other procedures that identify the key processes, stakeholders, roles and responsibilities and interested parties involved in the governance and management of the ISMS.	- Deploying a full set of governance processes with process definitions, stakeholder roles and responsibilities and flow charts will demonstrate the ISMS has the governance functions and management commitment required for effective risk management and certification.	Mid-term
IC4	The Chief Information Security Officer should develop a set of ISMS operational process flow charts or other procedures that identify the responsibilities of city resources and service providers involved in the deployment and operation of functional controls applicable to the ISMS.	- Creating a set of ISMS operational processes that cover the deployment and management of all key clauses of the functional controls in the ISO/IEC 27002 standard will provide a strong foundation for ensuring proper risk treatment of assets within the scope of the deployed ISMS.	Short-term

ISMS Evidence (IE): ISMS risk tracking and gap closure reporting need improvement.

#	Recommended Activity and Short Description	Expected Benefits	Time Frame
IE1	The Chief Information Security Officer should create a formal process for developing, reviewing and regularly updating the risk assessment, prioritization and risk treatment performed as part of the ISMS.	- Creating a formal process for risk assessment, prioritization and treatment will increase the overall consistency, effectiveness and visibility of the ISMS and the information protection it provides to city departments and create the documentation needed to support ISMS certification.	Short-term
IE2	The Chief Information Security Officer should create a more visible, comprehensive and timely tracking system for implementation plans, risk treatments and issue remediation activities of assets in the ISMS scope.	- Establishing a visible and complete tracking mechanism for ISMS activities will provide the information the Information Security Governance Board needs to more effectively identify project risks and other inherent risks that need to be prioritized, increasing the value of the ISMS.	Mid-term
IE3	The Chief Information Security Officer should create a formal mechanism in the ISMS or other department that will track corrective action plans to address audit issues identified for high-risk assets within the ISMS scope and regularly report on progress or deviations to the plans.	- Tracking audit issues for high-risk assets related to the ISMS will allow the Information Security Governance Board to have the information needed to properly prioritize, manage and track the corrective actions to closure.	Mid-term

Document Portfolio (DP): Some key ISMS documents are not released or readily available.

#	Recommended Activity and Short Description	Expected Benefits	Time Frame
DP1	The Chief Information Security Officer should establish a consistent ISMS documentation development, review, and approval process that includes identification, tracking and reporting of any open issues related to the ISMS documentation portfolio.	- Establishing a consistent ISMS document approval and release process, and a formal documentation portfolio management mechanism, will enable the ISMS team to focus on gaps in the portfolio required for ISO certification, and help the team determine and prioritize gap closure activities.	Short-term
DP2	The Chief Information Security Officer should develop a comprehensive inventory of policies, processes, procedures and guidance documents and an action plan to address the gaps in the ISMS and security controls policy portfolio in a timely manner.	- Creating a comprehensive inventory and gap closure plan for the ISMS documentation portfolio will increase consistency in roles and responsibilities, risk management, risk treatment and control deployments that impact information risk and ISMS compliance.	Mid-term
DP3	The Chief Information Security Officer should develop key policies to address information labeling and handling, and third-party user risk management.	- Developing policies for labeling and handling, and third-party risk management will provide the city with valuable tools to help employees and contractors understand their responsibilities and obligations related to information protection.	Mid-term

Issues Management (IM): Issues are tracked, but lack evidence of root cause analysis.

#	Recommended Activity and Short Description	Expected Benefits	Time Frame
IM1	The Chief Information Security Officer should create a list of all previously-identified security issues, vulnerabilities and other process weaknesses that have not been treated to determine the level of effort and action plans required to eliminate, mitigate, transfer or accept the risks.	- Identifying the inventory of latent issues that pose threats to City resources will help the Information Security Governance Board determine the inherent risk backlog that needs to be dealt with to achieve compliance.	Mid-term
IM2	The Chief Information Security Officer should create a formal process to document and track the risk rating, prioritization and treatment of all significant identified security issues that add to the level of inherent security risk of the city.	- Developing a process to track and address known issues to closure or acceptance provides assurance that new threats will be discovered and treated to avoid excessive adverse impact on city information resources and departments.	Mid-term
IM3	The Chief Information Security Officer should develop a vulnerability and risk management process that determines when and how data analytics and root cause analysis should be used for the identification and resolution of issues.	- Properly incorporating data analytics and root cause analysis in the management of risks will reduce the potential for issues to become chronic or for latent issues to remain long enough to pose an extreme risk to city assets.	Short-term

ISMS Reporting (IR): Current reporting is not sufficient to track and drive change.

#	Recommended Activity and Short Description	Expected Benefits	Time Frame
IR1	The Chief Information Security Officer should analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate, to provide useful information to each audience.	- Ensuring metrics provide tangible value to an executive, management and/or operational audience increases the quality and effectiveness of risk and control decisions, and reduces wasted efforts associated with meaningless metrics.	Short-term
IR2	The Chief Information Security Officer should identify and create ISMS Program Metrics that measure and report key success criteria and progress against the goals of the ISMS.	- Regularly reporting program-level metrics for the ISMS will provide management and stakeholders the information needed to determine the effectiveness of the ISMS.	Short-term
IR3	The Chief Information Security Officer should create a deep-dive analysis process that mandates identifying root causes and remediation actions to eliminate large-scale, chronic issues (e.g., Rapid7 vulnerabilities).	- A formal process that can be activated when needed as a point of escalation for critical or chronic problems will ensure critical and severe issues will be dealt with on a timely basis, reducing the overall risk level of the organization.	Short-term
IR4	The Chief Information Security Officer identify and implement key Executive, Management and Operational ISMS Metrics that will be most useful for each stakeholder.	- Identifying and deploying appropriate information security metrics will provide each stakeholder the information needed to better understand and manage information risks and protection.	Short-term

Strategic Focus (SF): The ISMS needs a more visible focus on managing strategic risks.

#	Recommended Activity and Short Description	Expected Benefits	Time Frame
SF1	The Chief Information Security Officer should develop an ISMS Annual Plan that provides a single view of identified strategic initiatives to improve the ISMS and known (or proposed) tactical remediation activities	- Creating a comprehensive plan for the ISMS and related services that provides a long-term outlook and is regularly reviewed will help drive commitment and resource allocation	Mid-term
SF2	The Chief Information Security Officer should create a tracking mechanism that captures and reports on the annual plan initiatives and activities approved by the Information Security Governance Board, as well tracking deviations (positive or negative) from the plan.	- Publishing a regular status report of strategic and tactical initiatives helps drive consistent understanding of overall priorities and reduces many forms of program slippage.	Mid-term
SF3	The Chief Information Security Officer should review the potential need for a separate Tactical ISMS Activities report that provides a status of short- and medium-term activities while the ISMS is still in its developmental stage.	- The implementation phase of the ISMS will include a lot of tactical and very short-term activities that have interdependencies with subsequent activities; providing a visible means to identify any deviations in delivery is critical to avoiding program slippage.	Short-term

Program Resourcing (PR): The ISMS initiative lacks sufficient resources to meet the expected certification timeframe.

#	Recommended Activity and Short Description	Expected Benefits	Time Frame
PR1	The Chief Information Security Officer should conduct a comprehensive resource and skills analysis of the Office of Information Security to identify gaps in the appropriate level of security resources required to fully implement and operate the ISMS.	- Understanding the resource requirements and assigning adequate resources will help the City to complete the implementation activities required for the ISMS to be completed and prepared for certification.	Short-term
PR2	The Chief Information Security Officer should conduct a study to determine if additional resourcing is required in the Office of Information Security peer groups and business units to complete the implementation of the ISMS and effectively oversee its operation.	- Assigning adequate security support and peer group staffing resources will help the City in implementing a certifiable ISMS program.	Mid-term
PR2	The Chief Information Security Officer should create a resourcing plan to allocate appropriate resources to complete the tasks identified in the ISMS project plan and gap remediation plans with a goal of full resourcing in CY2017.	- Allocating the appropriate resources to meet the needs of the agreed project plan will enable the City of Atlanta to implement an ISMS that fully supports the security needs of the City.	Short-term

Appendix B: Management Review and Response to Audit Recommendations

Report #17.06	Report Title: ISO/IEC 27001 ISMS Pre-Certification Audit	Date: Nov 2017
Recommendation Responses		
Rec. 1	The Chief Information Security Officer should create and deploy a single scope statement that will clarify, document and communicate a common, approved City of Atlanta ISO certification scope to all affected parties.	Agree
<p><u>Proposed Action:</u> Validate Scope with CIO (Chief Information Officer) & CISO (Chief Information Security Officer) and recommunicate single scope statement to all stakeholders.</p> <p><u>Implementation Timeframe:</u> FY18 – Q3</p> <p><u>Comments:</u> Leverage remaining hours with existing contracts to support completion of these activities.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 2	The Chief Information Security Officer should determine and execute corrective actions to close any gaps in the existing policies and/or procedures needed to cover the ISO/IEC 27001/2 domains and clauses included in the Statement of Applicability for assets within the scope of the ISMS.	Agree
<p><u>Proposed Action:</u> Perform gap analysis and validate statement of applicability for the ISMS program.</p> <p><u>Implementation Timeframe:</u> FY18 – Q3</p> <p><u>Comments:</u> Leverage remaining hours with existing contracts to support completion of these activities.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 3	The Chief Information Security Officer should develop a set of ISMS process flow charts or other procedures that identify the key processes, stakeholders, roles and responsibilities and interested parties involved in the governance and management of the ISMS.	Agree
<p><u>Proposed Action:</u> Define key processes that require flowcharting and procedures for this recommendation and develop the documentation to support this improvement.</p> <p><u>Implementation Timeframe:</u> FY18 – Q4</p> <p><u>Comments:</u> Leverage remaining hours with existing contracts to support completion of these activities.</p> <p><u>Responsible Person:</u> CISO</p>		

Rec. 4	The Chief Information Security Officer should develop a set of ISMS operational process flow charts or other procedures that identify the responsibilities of city resources and service providers involved in the deployment and operation of functional controls applicable to the ISMS.	Agree
<p><u>Proposed Action:</u> Define key operational processes that require flowcharting and procedures for this recommendation and develop the documentation to support this improvement.</p> <p><u>Implementation Timeframe:</u> FY18 – Q4</p> <p><u>Comments:</u> Need to understand expected output; Leverage remaining hours w/existing contracts to support completion of these activities.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 5	The Chief Information Security Officer should create a formal process for developing, reviewing and regularly updating the risk assessment, prioritization and risk treatment performed as part of the ISMS.	Agree
<p><u>Proposed Action:</u> Create formal process for ISMS risk management to include but not be limited to annual assessment, prioritization and treatment as approved by our CISO/CISO/Business Decision Makers; require assessment for new systems, annual review of existing systems, and assessment based on changes to production submitted via AIM’s change advisory board (Reference: Risk Based Scorecard on Applications).</p> <p><u>Implementation Timeframe:</u> FY19</p> <p><u>Comments:</u> Resource Risks are associated with implementing these activities within current fiscal year; timeline being evaluated.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 6	The Chief Information Security Officer should create a more visible, comprehensive and timely tracking system for implementation plans, risk treatments and issue remediation activities of assets in the ISMS scope.	Agree
<p><u>Proposed Action:</u> Create Office of Information Security (OIS) Action Item Portal to track actions required from the Information Security Governance Board (ISGB), Internal Audit and vulnerability reports for completions/audit/compliance improvements.</p> <p><u>Implementation Timeframe:</u> FY18 – Q4</p> <p><u>Comments:</u> Portal in Beta Testing 9/2017; full rollout by FY18 - Q2</p> <p><u>Responsible Person:</u> CISO</p>		

Rec. 7	The Chief Information Security Officer should create a formal mechanism in the ISMS or department that will track corrective action plans to address audit issues identified for high-risk assets within the ISMS scope and regularly report on progress or deviations to the plans.	Agree
<p><u>Proposed Action:</u> Create OIS Action Item Portal to track actions required from ISGB, Internal Audit and vulnerability reports for completions/audit/compliance improvements.</p> <p><u>Implementation Timeframe:</u> FY18 – Q4</p> <p><u>Comments:</u> Portal in Beta Testing 9/2017; full rollout by FY18 - Q2</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 8	The Chief Information Security Officer should establish a consistent ISMS documentation development, review, and approval process that includes identification, tracking and reporting of any open issues related to the ISMS documentation portfolio.	Agree
<p><u>Proposed Action:</u> Validate document management plan to include management of version control of documentation, review and signoff requirements, customer visible versions vs team visibility into all versions. Include use of OIS Action Tracking Portal for ISGB/Audit as key activity and define what's in scope for portal vs. other OIS tools.</p> <p><u>Implementation Timeframe:</u> FY18-Q4</p> <p><u>Comments:</u> Possible resource constraints</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 9	The Chief Information Security Officer should develop a comprehensive inventory of policies, processes, procedures and guidance documents and an action plan to address the gaps in the ISMS and security controls policy portfolio in a timely manner.	Agree
<p><u>Proposed Action:</u> Consolidate information into primary ISGB site integrate with OIS team site; replicating date where appropriate.</p> <p><u>Implementation Timeframe:</u> FY18-Q4</p> <p><u>Comments:</u></p> <p><u>Responsible Person:</u> CISO</p>		

Rec. 10	The Chief Information Security Officer should develop key policies to address information labeling and handling, and third-party user risk management.	Agree
<p><u>Proposed Action:</u> Review information classification policy to be sure language covers audit recommendation. Incorporate into annual policy update to processes and procedures.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u></p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 11	The Chief Information Security Officer should create a list of all previously-identified security issues, vulnerabilities and other process weaknesses that have not been treated to determine the level of effort and action plans required to eliminate, mitigate, transfer or accept the risks.	Agree
<p><u>Proposed Action:</u> Implementation OIS Action Tracking Portal to include requirements from this recommendation and incorporate into Vulnerability Review Board (VRB).</p> <p><u>Implementation Timeframe:</u> FY18 Q3</p> <p><u>Comments:</u> Consolidate existing systems and categorize for ease of tracking and reporting.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 12	The Chief Information Security Officer should create a formal process to document and track the risk rating, prioritization and treatment of all significant identified security issues that add to the level of inherent security risk to the city.	Agree
<p><u>Proposed Action:</u> Define, validate and Incorporate into APMS and make any necessary adjustments to Risk-Based Business Scorecard (RBBS) and Applications Portfolio Management System (APMS) as appropriate.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u> System is developed and risk formula has been incorporated into the system; process needs to be validated through RBBS project as a requirement.</p> <p><u>Responsible Person:</u> CISO</p>		

Rec. 13	The Chief Information Security Officer should develop a vulnerability and risk management process that determines when and how data analytics and root cause analysis should be used for the identification and resolution of issues.	Agree
<p><u>Proposed Action:</u> Define, validate and Incorporate into VRB and make any necessary adjustments to RBBS and APMS as appropriate.</p> <p><u>Implementation Timeframe:</u> FY18 Q3</p> <p><u>Comments:</u> Update current Vulnerability Mgt. Process to include RCA as output of process.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 14	The Chief Information Security Officer should analyze the portfolio of current metrics for the value each provides, and add, adjust, or discard metrics, as appropriate, to provide useful information to each audience.	Agree
<p><u>Proposed Action:</u> Define, validate and incorporate into VRB and make any necessary adjustments to ISMS, as appropriate.</p> <p><u>Implementation Timeframe:</u> FY18 Q2</p> <p><u>Comments:</u> Updated and completed; new metrics approved by ISGB in FY18 Q2</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 15	The Chief Information Security Officer should identify and create ISMS Program Metrics that measure and report key success criteria and progress against the goals of the ISMS.	Agree
<p><u>Proposed Action:</u> Define, validate and incorporate into ISMS and make any necessary adjustments to other artifacts, as appropriate.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u> Review and confirm that we've included the following metrics: security awareness training metrics; mean time to resolution (MTTR); phishing results; define metrics for Risk Based Business Scorecard (RBBS) to incorporate into this response; use metrics from Rec.14 and validate against goals.</p> <p><u>Responsible Person:</u> CISO</p>		

Rec. 16	The Chief Information Security Officer should create a deep-dive analysis process that mandates identifying root causes and remediation actions to eliminate large-scale, chronic issues (e.g., Rapid7 vulnerabilities).	Agree
<p>Proposed Action: Define, validate and incorporate requirements into VRB and incident management improvements; make any necessary adjustments to RBBS and APMS as appropriate.</p> <p>Implementation Timeframe: FY18 Q4</p> <p>Comments: Add root cause analysis (RCA) process to vulnerability management process.</p> <p>Responsible Person: CISO</p>		
Rec. 17	The Chief Information Security Officer should identify and implement key Executive, Management and Operational ISMS Metrics that will be most useful for each stakeholder.	Agree
<p>Proposed Action: Define, validate and Incorporate in to ISGB and make any necessary adjustments to other artifacts, as appropriate.</p> <p>Implementation Timeframe: FY18 Q2</p> <p>Comments: Metrics were adopted by executive stakeholders and approved in FY18 Q2 Board meeting.</p> <p>Responsible Person: CISO</p>		
Rec. 18	The Chief Information Security Officer should develop an ISMS Annual Plan that provides a single view of identified strategic initiatives to improve the ISMS and known (or proposed) tactical remediation activities.	Agree
<p>Proposed Action: Incorporate IS tactical plan as part of the OIS Strategic Plan and ISMS Annual Plan.</p> <p>Implementation Timeframe: FY19</p> <p>Comments: In Progress</p> <p>Responsible Person: CISO</p>		

Rec. 19	The Chief Information Security Officer should create a tracking mechanism that captures and reports on the annual plan initiatives and activities approved by the Information Security Governance Board, as well tracking deviations (positive or negative) from the plan.	Agree
<p><u>Proposed Action:</u> Add to tracking portal as action for each year; update annually.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u> In progress; portal created.</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 20	The Chief Information Security Officer should review the potential need for a separate Tactical ISMS Activities report that provides a status of short- and medium-term activities while the ISMS is still in its developmental stage.	Agree
<p><u>Proposed Action:</u> Utilize tactical plan outlined in the Cyber Response Executive Report. Validate ISMS Plan and incorporate IS tactical plan as part of the plan; validate what's required for the activities report since we track action log, strategic plan reviews and project based reviews.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u> Ref: Rec.#19;</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 21	The Chief Information Security Officer should conduct a comprehensive resource and skills analysis of the Office of Information Security to identify gaps in the appropriate level of security resources required to fully implement and operate the ISMS.	Agree
<p><u>Proposed Action:</u> Submit proposed OIS Reorganization request for additional resources.</p> <p><u>Implementation Timeframe:</u> FY18 Q3</p> <p><u>Comments:</u> Prioritize this effort to incorporate into FY19 ask; work in progress.</p> <p><u>Responsible Person:</u> CISO</p>		

Rec. 22	The Chief Information Security Officer should conduct a study to determine if additional resourcing is required in the Office of Information Security peer groups and business units to complete the implementation of the ISMS and effectively oversee its operation.	Agree
<p><u>Proposed Action:</u> Submit proposed OIS Reorganization request for additional resources.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u> See Rec. #21</p> <p><u>Responsible Person:</u> CISO</p>		
Rec. 23	The Chief Information Security Officer should create a resourcing plan to allocate appropriate resources to complete the tasks identified in the ISMS project plan and gap remediation plans with a goal of full resourcing in CY2017.	Agree
<p><u>Proposed Action:</u> Plan to be proposed in FY18 and implemented by FY19.</p> <p><u>Implementation Timeframe:</u> FY18 Q4</p> <p><u>Comments:</u> See Rec. #21</p> <p><u>Responsible Person:</u> CISO</p>		

Appendix C: ISO/IEC 27001/2 Control Objectives and Control Clauses

ISO/IEC 27001:2013 Management Control Objectives and Control Clauses

4. Context of the organization

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the information security management system
- 4.4 Information security management system

5. Leadership

- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

6. Planning

- 6.1 Actions to address risk and opportunities
- 6.2 Information security objectives and plans to achieve them

7. Support

- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8. Operation

- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

9. Performance evaluations

- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10. Improvements

- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

ISO/IEC 27002:2013 Management Control Objectives and Control Clauses

14 Domains; 35 Control Objectives; 114 controls

5. Information Security Policies

5.1 Management direction for information security

6. Organization of information security

6.1 Internal organization

6.2 Mobile devices and teleworking

7. Human resource security

7.1 Prior to employment

7.2 During employment

7.3 Termination and change of employment

8. Asset management

8.1 Responsibility for assets

8.2 Information classification

8.3 Media handling

9. Access control

9.1 Business requirements of access control

9.2 User access management

9.3 User responsibilities

9.4 System and application access control

10. Cryptography

10.1 Cryptographic controls

11. Physical and environmental security

11.1 Secure areas

11.2 Equipment

12. Operations security

12.1 Operational procedures and responsibilities

12.2 Protection from malware

12.3 Backup

12.4 Logging and monitoring

12.5 Control of operational software

12.6 Technical vulnerability management

12.7 Information systems audit considerations

13. Communications security

13.1 Network security management

13.2 Information transfer

14. System acquisition, development and maintenance

14.1 Security requirements of information systems

14.2 Security in development and support processes

14.3 Test data

15. Supplier relationships

15.1 Information security in supplier relationships

15.2 Supplier service delivery management

16. Information security incident management

16.1 Management of information security incidents and improvements

17. Information security aspects of business continuity management

17.1 Information security continuity

17.2 Redundancies

18. Compliance

18.1 Compliance with legal and contractual requirements

18.2 Information security reviews