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 it's 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- missing or outdated policies, procedures and guidance documents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	