BOARD OF DIRECTORS

METROPOLITAN ATLANTA RAPID TRANSIT AUTHORITY

AUDIT COMMITTEE

THURSDAY, MARCH 18, 2021

ATLANTA, GEORGIA

via WebEx

MEETING MINUTES

Committee Chair Freda Hardage called the meeting to order at 10:35 a.m.

Board Members Present	Staff Members Present
Roberta Abdul-Salaam	Jeffrey Parker
Robert Ashe	Collie Greenwood
Stacy Blakley	Luz Borrero
William Floyd	Elizabeth O'Neill
Roderick Frierson	Melissa Mullinax
Freda Hardage, **Chair**	Raj Srinath
Rita Scott	

Also, in attendance: MARTA Board General Counsel Justice Leah Ward Sears of Smith, Gambrell & Russell, LLP; other MARTA staff members: Dean Mallis, Kirk Talbott, Marsha Anderson Bomar, Santiago Osorio, Patricia Lucek, M Scott Kreher, Emil Tzanov, Rhonda Allen, Kevin Hurley, Paula Nash, Tyrene Huff and Jaquata Jordan.

Approval of the November 20, 2020 Audit Committee Meeting Minutes

On motion by Committee Chair Hardage, seconded by Board member Frierson, the minutes were unanimously approved by a vote of 7 to 0, with 7 members present.

Resolution Authorizing a Modification in Contractual Authorization for Professional Services for an Internal Audit GRC Automation Tool, LOA L46790

Mr. Tzanov presented the resolution to the committee. The ACL Services, LTD GRC software cloud platform/tool is the system of record for the MARTA Department of Internal Audit ("IA"). It is currently being used by IA to plan, project-manage, document, and report all audit engagements. Further, this tool is a critical component and enabler of the IA's Continuity of Operations ("COOP") plan and is documented accordingly in Tab A/Annex 15 of the MARTA COOP plan.

Mr. Tzanov stated that the original contract value was $77,000.00 for a one (1) year term; however, the Authority is modifying the contract to extend the term to April 23, 2024 and increase the contract value to $310,916.00.

Mr. Tzanov requested approval of the resolution. Committee Chair Hardage asked the Board for a motion for approval. The motion was granted by Board member Ashe and seconded by Board member Frierson.

Board member Frierson asked if the software platform included all audits throughout the enterprise or just done internally. Mr. Tzanov stated that it was used only for Internal Audit Engagements.

The resolution was unanimously approved by a vote of 7 to 0, with 7 members present.

Internal Audit Activity Briefing ***[Presentation attached]***

Mr. Tzanov provided an overview on the audits completed during the period.

COVID Related Audits

- Cleaning of Breeze machines (TVMs) and other high touch areas at rail stations (related to COVID-19)- COMPLETED
- Cleaning of buses based on COVID-19 and other relevant SOPs- COMPLETED
- Cleaning & disinfectant supplies availability (related to COVID-19) and proactive ordering procedures- COMPLETED
- Integrated Operations Center (IOC) Safety Procedures (related to COVID-19) - COMPLETED

The Department of Internal Audit has three (3) Audit Branches:

- Operations Audit Group
- Contracts Audit Group
- Information Technology Audit Group

Mr. Tzanov stated that the Operational Audit group issued 3 audits.

1) Capital Improvement Program – Follow Up Audit
   - Initial 2017 audit identified 28 Findings
   - The current follow-up audit noted:
   - 18 recommendations had been implemented
   - 10 recommendations are in the process of implementation with expected completion date of June 30, 2021

2) Cubic-Automated Fare Collection System
   - In Report Writing phase

3) Covid-19 Expenditure Audit
   - Undergoing Fieldwork

Mr. Tzanov continued discussing upcoming internal audit Covid-19 Advisory reviews. He stated that the internal audit office will continue to assist the Authority in standard

operating procedures regarding Covid-19. This will include Review of Replacement of Cabin Air Filters – Bus Fleet. Also Review of Replacement of Rail Car Air Filters – Rail fleet. As well as the Installation of Needle Point Filtration Systems at MARTA facilities.

Mr. Tzanov spoke on prior audits with open findings. The Vertical Transportation audit findings will be completed by the May audit committee meeting. The Physical Security Bus & Rail facilities has 3 findings that have been completed with 2 in process.

Mr. Tzanov stated there are several other audits with open findings for a total of 18 that are still in the process of being completed. There is one that is past due but should be completed by the next audit committee meeting.

Mr. Tzanov continued his discussion for Information Technology Audit. The Cubic Automated Fare collection system is in the report writing phase. The Software Patch management audit is currently in the planning phase.

Mr. Tzanov continued speaking on prior audits with open findings in the IT Audit Group. Currently the total significant & moderate findings are 17, 7 which are closed, 4 in process and 6 past due.

Mr. Tzanov stated that the Contract Audit group completed 14 audits. They identified $1.1m in unallowable cost in overhead rate reviews per federal acquisition regulation. In addition to that, there was $287k identified potential cost savings in Cost/Price and change order reviews.

Mr. Tzanov spoke about Fraud, Waste, & Abuse. There were only 2 calls received on the hotline from October 1, 2020 to January 31, 2021.

Other Matters

Mr. Tzanov spoke on personnel within the department. He stated that there are currently 16 approved/budgeted positions. 3 positions need to be filled permanently. There is currently 1 “Open records” request received from WSB/ Richard Belcher for all 2020 Operational Audit reports.

Cyber Security Update ***[Presentation attached]***

Dean Mallis, AGM of Information Security/CISO, gave an update on the Cybersecurity program.

Mr. Mallis stated that the Authority recently implemented malicious domain blocking and reporting. This is a free service from the Department of Homeland Security. It helps block up to 90% of ransomware attacks. Upgrade to paid version which will provide the following: security for remote users, enforce security policies, security alert investigations, website filtering, customizable reports. ~43k a year. Mr. Mallis stated that the security awareness training is about 89% completed. Microsoft Sentinel was implemented which is a log aggregator for Microsoft products.

Mr. Mallis stated that the multifactor authentication rollout will continue and is expected to be completed by March 31st.

Mr. Mallis spoke about the implementation of a security switch replacement and anti-virus replacement systems. Both are on target for June/July 21. SIEM/ Vulnerability Scanner/Managed services/additional endpoint protection (remote users) deals with replacing existing SIEM (security information and event management), vulnerability scanner, network monitoring with an outsourced vendor. True 24/7/365 coverage frees up FTE to work on threat hunting.

Mr. Mallis stated that there will be an implementation of a Microsoft cloud app security, train control cyber security monitoring, data loss protection (DLP), and penetration test application.

Board member Frierson asked if the push campaign (Phishing test) is done across the entire enterprise. Mr. Mallis stated that everyone is subject to testing, including senior leadership.

Board member Frierson asked how many emails go out. Mr. Mallis stated that it was about 3500 to 4000 emails that go out.

Board member Frierson asked how the password updates are handled with Microsoft. Mr. Mallis stated that the Authority is on a 90-day cadence to reset passwords.

Adjournment

The Committee meeting adjourned at 12:08 a.m.

Respectfully submitted,

Jaquata Jordan

Jaquata Jordan
Department Administrator, Audit

YouTube Link: https://youtu.be/TFKyySy0L2M

Internal Audit Activity Briefing

(10/01/2020 – 01/31/2021)

Internal Audit Department (current period)

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Cleaning of Breeze machines (TVMs) and other high touch areas at rail stations (related to COVID-19)	01/23/21	Advisory	**Completed**	Advisory Engagement / Recommendation Made							
Cleaning of buses based on COVID-19 and other relevant SOPs	01/23/21	Advisory	**Completed**	Advisory Engagement / Recommendation Made							
Cleaning & disinfectant supplies availability (related to COVID-19) and proactive ordering procedures	01/23/21	Advisory	**Completed**	Advisory Engagement / Recommendation Made							
Integrated Operations Center (IOC) Safety Procedures (related to COVID-19)	01/23/21	Advisory	**Completed**	Advisory Engagement / No Recommendations							

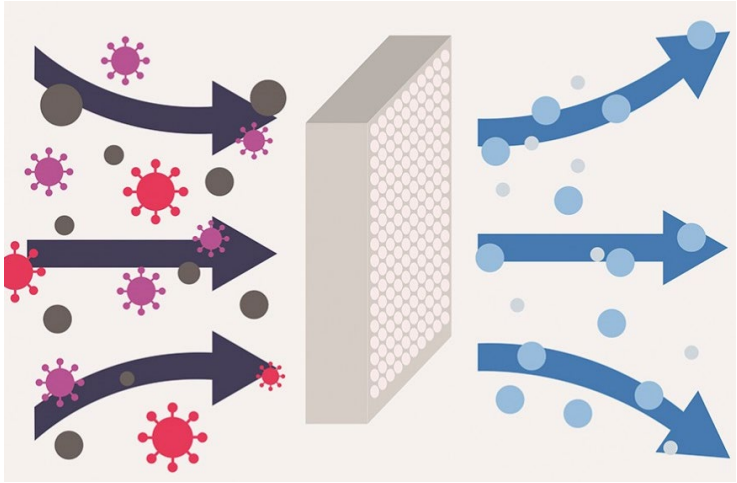
Operational Audit Group *(current period)*

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Capital Improvement Program – Follow Up Audit	01/15/2021	Follow-up Audit (Low Risk)	**Completed**	• Initial 2017 audit identified 28 Findings • The current follow-up audit noted: ○ 18 recommendations had been implemented ○ 10 recommendations are in the process of implementation with expected completion date of June 30, 2021.							
Cubic-Automated Fare Collection System *	Q3	TBD	**Report Writing**	-	-	-	-	-	-	-	-
Covid-19 Expenditure Audit	Q3	TBD	**Fieldwork**	-	-	-	-	-	-	-	-

* *Integrated audit with the IT Audit Branch*

Upcoming Internal Audit Covid-19 Advisory Reviews (Q3)

- Replacement of cabin air filters – bus fleet
- Replacement of rail car air filters – rail fleet
- Installation of needle point filtration systems at MARTA facilities



Operational Audit Group – Prior Audits with Open Findings

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Vertical Transportation Contract Management	06/30/20	High Risk	Completed	4	-	4	-	2	-	2	-
- *Failure to perform periodic testing of elevators & escalators (05/01/2021)* - *Untimely preventative maintenance of elevators & escalators (05/01/2021)* - *Failure to clean elevator & escalator units (05/01/2021)* - *Inadequate manpower as required by contract (05/01/2021)*											
Physical Security of Bus & Rail Facilities	3/31/20	High Risk		5	3	2	-	-	-	-	-
- MARTA Bus & Rail facilities lack documented security procedures. (05/30/21) - Physical Security at MARTA facilities needs improvement. (05/30/21)											

Operational Audit Group – Prior Audits with Open Findings *(cont.)*

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
I-Supplier and Direct Pay	12/31/19	High	Completed	5	4	1	-	-	-	-	-
- Management's Action Plans from prior audits have not been implemented. *(IA verifying completion)*											
Drug and Alcohol Policy Enforcement	4/5/19	Needs Attention	Completed	1	-	1	-	3	2	1	-
- *Enhance Zone Bus Supervisor coverage on bus routes which do not enter a station with an assigned bus supervisor. (05/01/2021)*											
Direct Pay Process	10/31/18	High Risk	Completed	3	1	1	1	-	-	-	-
- Drive *stronger enforcement of procurement procedures for purchasing goods/services in non-exempt direct pay categories. (IA verifying completion)* - *Enhance and automate the External Training Request Form through Oracle. (7/1/19)*											
HR Resources/Talent Acquisition Process and HR General Controls	10/29/18	Needs Attention	Completed	-	-	-	-	2	1	-	1
Total Significant & Moderate Findings:				***18***	***8***	***9***	***1***	***7***	***3***	***3***	***1***

Information Technology Audit Group (current period)

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
Cubic-Automated Fare Collection System *	Q2	TBD	**Report Writing**	-	-	-	-	-	-	-	-
Software Patch Management	Q3	TBD	**Planning**	-	-	-	-	-	-	-	-

* *Integrated audit with the Operational Audit Branch*

IT Audit Group – Prior Audits with Open Findings

Audit Title	Audit Report Issue Date	Audit Engagement Rating	Audit Project Status	Significant Findings				Moderate Findings			
				Total	Closed	In Process	Past Due	Total	Closed	In Process	Past Due
AVIS Controller Software	08/07/20	High Risk	Completed	4	2	0	2	-	-	-	-
- Controls to detect software security vulnerabilities were not adequately implemented, which increases the risk of malicious disruption (9/30/2020) - The project was lacking appropriate personnel in key roles, which diminished the effectiveness of oversight (10/31/20)											
Mobile Ticketing	07/15/20	High Risk	Completed	2	-	-	2	1	-	1	-
- Project management controls not adequately implemented, which increases the risk of missing implementation target dates (09/30/20) - Software defects identified during testing were not resolved timely, which has delayed the realization of project benefits (09/30/20).											
TCS & SCADA – Cybersecurity	3/09/20	High Risk	Completed	6	2	4	-	1	-	1	-
- Proactive detection of technical vulnerabilities was not adequately managed. (09/01/21) - User access management controls were not designed or implemented effectively. (04/09/21) - Cybersecurity monitoring controls were not implemented. (09/01/21) - Training per the contract was not developed or delivered, impairing MARTA personnel's ability to administer the system. (05/06/21)											
Cybersecurity – PCs, Email and Internet	6/24/19	High Risk	Completed	5	3	-	2	3	1	-	2
- Not all end user devices on the MARTA network were centrally managed. (1/31/20) - Devices were running unsupported software, which increases the risk of vulnerabilities being exploited. (5/31/20)											
Total Significant & Moderate Findings:				**17**	**7**	**4**	**6**	**5**	**1**	**2**	**2**

Contracts Audit Group

Audits Completed This Period (10/1/2020 – 1/31/2021)	
Audit Opinions	Audits Issued
Low Risk	12
Needs Attention	2
Total Audits Issued	14
Identified Unallowable Cost in Overhead Rate Reviews per Federal Acquisition Regulation ("FAR")	$1,111,549
Identified Potential Cost Savings in Cost/Price and Change Order Reviews	$287,708

Audits In Progress	
Audit Types	
Interim/Close Out	1
Rate Reviews	13
Cost/Price Analysis	1
Change Orders Special Audit (Incurred Cost, Special Request, Buy America & Claims)	1
Total Contract Audits in Progress	**16**

Fraud, Waste & Abuse (“FWA”) Summary

- 2 calls received on the FWA hotline from October 1, 2020 to January 31, 2021
  - 1 call (50%) requested a callback. The callback determined that the caller's issue had been resolved.
  - 1 call (50%) was forwarded to customer service for resolution.

Other Matters

- Personnel Update
  - 16 Approved/budgeted positions
  - Three positions need to be filled permanently
    - IT Audit Manager – vacant
    - Senior Auditor – vacant
    - Director of Operational Audit & Fraud Investigations – Charles Middlebrooks serving as Acting Director

- One “Open Records” request received from WSB / Richard Belcher for all 2020 Operational Audit reports

APPENDIX

Contracts Audit Group: Audit Types

COST/PRICE ANALYSIS

Objective: To ensure the Contractor's proposed cost/price is fair and reasonable.

FORWARD PRICING AUDIT

Objective: To determine/recommend the rates and factors for overhead rates, equipment, and profit that will govern future change orders.

CHANGE ORDER AUDIT

Objective: To ensure the proposed increase or decrease of the price of the contract is fair and reasonable.

CLOSEOUT AUDIT

Objective: To ensure the contract was executed in accordance with MARTA's policies and procedures and to verify the funds expended.

RATE REVIEW

Objective: To ensure the following:

- The Contractor's accounting system is considered adequate to (a) identify, account for, record, and accumulate project costs, and (b) identify and segregate direct and indirect costs on a consistent basis.
- The company is financially capable of performing the work required under the contract.
- The labor rates proposed are reasonable.
- The overhead rate proposed is allowable, allocable, reasonable, and in accordance with the Federal Acquisition Regulations.

INCURRED COST/TRUE UP AUDIT

Objective: To verify expended amounts and to ensure the funds were expended in accordance with MARTA procedures.

BUY AMERICA AUDIT

Objective: To ensure that during the procurement of rolling stock; including train control, communication, traction power equipment, and rolling stock prototypes, the costs of the components and subcomponents produced in the US meet or exceed Federal guidelines.

Overall Audit Engagement Opinion

on the system of internal controls related to the scope of the audit engagement

Opinion Rating	Conclusion
"Low Risk"	• Minimal or no findings noted in the report. • Significant risk related activities are adequately controlled. • Management's control environment appears sound, with minimal or no exceptions. • The Agency is in compliance with all applicable laws and regulations. • For Contract Audits, the noted deficiencies, in aggregate, amount to less than $50,000, or 10% of the total contract value, whichever is lower.
"Needs Attention"	• Control environment impairment exists that may have moderate impact on MARTA. • Significant risk related activities are not adequately controlled. • No more than one finding is rated as "Significant". • Immediate safety and soundness are not threatened, but the control environment requires improvement. • Minor non-compliance with applicable laws and regulations may exist. • Exposure to fraud or security vulnerabilities exist. • For Contract Audits: the noted deficiencies, in aggregate, amount to less than $200,000 or 50% of the total contract value, whichever is lower.
"High Risk"	• The control environment is not adequate and below standard. • Two or more findings are rated as "Significant". • Major financial losses, operational impact, or reputational damage may occur. • Significant exposure to fraud or security vulnerabilities exist. • Requires the General Manager's immediate attention. • For Contract Audits: the noted deficiencies, in aggregate, exceed $200,000 or 50% of the total contract value, whichever is lower.

Risk Rating of Individual Reported Findings

Finding Rating	Risk Impact

Significant	**Risk has a high impact and likelihood**
	• A high priority issue exists. Immediate attention from the functional or operational Assistant General Manager is required.
	• Serious internal control or risk management issues exist that, if not mitigated, may result in:
	  ○ Substantial losses, possibly in conjunction with other weaknesses in the internal control. environment of the process being audited or MARTA as a whole.
	  ○ Serious violation of MARTA's strategies, policies, or values.
	  ○ Serious reputation damage.
	  ○ Significant adverse regulatory impact, such as loss of operating licenses or material fines.

Moderate	**Risk has a high impact and low likelihood, or low impact and high likelihood**
	• A medium-priority issue exists.
	• Timely attention from the functional or operational Assistant General Manager is necessary.
	• An internal control or risk management issue could lead to:
	  ○ Financial losses.
	  ○ Loss of controls within the audited operating unit, function, process, or MARTA.
	  ○ Reputation damage.
	  ○ Adverse regulatory impact, such as public sanctions or fines.

Low	**Risk has a low impact and low likelihood** • A low priority issue exists. • Routine attention from the Assistant General Manager or line management is expected. • A minor internal control or risk management deficiency exists, the remediation of which may lead to improvement in the quality or efficiency of MARTA, the operating unit, function, or process being audited. • Risks are limited.

Information Security Update March 2021

marta

Information Security Implementation Roadmap

SolarWinds breach – MARTA was not impacted – Highlights need for improved monitoring

Malicious Domain Blocking and Reporting Deployed - Free
Malicious Domain Blocking and Reporting, or MDBR, service works by preventing IT devices from connecting to web domains known to be affiliated with ransomware, other forms of malware, phishing campaigns and other threats.

- Upgrade to paid version which will provide the following: security for remote users, enforce security policies, security alert investigations, website filtering, customizable reports. ~43k a year.

Phishing Campaign 1 - completed – 10.3% phish rate. Industry standard is 27.2%
Phishing Campaign 2 – completed – 9.4% phish rate – .9% decrease
Phishing campaign tests the effectiveness of cyber security awareness training

Security Awareness Training – 89% completed the training.

Microsoft Sentinel – Free components implemented – log aggregator for Microsoft products

Multifactor Authentication (MFA) – rollout continues. Projected completion March 31st
Verifies user identity by requiring multiple credentials rather than relying only on usernames and passwords.

- Require MFA for all users accessing MARTA cloud services externally
- Forthcoming Requiring MFA for administrative role functions across the environment

Information Security Implementation Roadmap

Security switch replacement (IT) – grant funding

Replace aging infrastructure
allows blocking of unauthorized devices

Anti-virus replacement –on target for June/July 21

Replace existing implementation with an advanced endpoint protection.

SIEM/Vulnerability Scanner/Managed services/additional endpoint protection (remote users)

Replace existing SIEM (security information and event management), vulnerability scanner, network monitoring with an outsourced vendor. True 24/7/365 coverage, Frees up FTE to work on threat hunting.

Grant funding - Will close out FY17 1-million-dollar grant.

Microsoft Cloud App Security

Provides risk analysis, cloud discovery, behavioral analytics, data protection, and threat protection.

Train control cyber security monitoring – 21/22

Possible grant funding for initial procurement. – real-time monitoring tool

Data Loss Protection (DLP) - 2022

Identifies/monitors/protects sensitive information across Marta's cloud and end user environments, prevents accidental sharing of sensitive information, helps users learn how to stay compliant without interrupting their workflow and creates reports showing content that matches MARTA's DLP policies.

Penetration test – applications.

Information Security Implementation Roadmap

Self-Assessment of Critical Security Control to NIST 800-53 Rev-4				
CSC ID	**Critical Security Controls**	**CIS Control Status**	**% Implemented**	**Comments**
CSC #1	Inventory of Authorized and Unauthorized Devices	Planned	0%	
CSC-#2	Inventory of Authorized and Unauthorized Software	Planned	0%	
CSC #3	Continuous Vulnerability Assessment and Remediation	In Progress	70%	Monthly and ongoing vulnerability scans are run both internally and externally and continuous monitoring is ongoing with Plunk and other security tools.
CSC #4	Controlled Use of Administrative Privileges	In Progress	60%	Policy has been revised. Information security will keep working with IT to ensure best practices for privilege access
CSC #5	Secure Configurations for Hardware and Software	In Progress	60%	Policy has been revised. Information security will keep working with IT to ensure more secure configuration
CSC #6	Maintenance, Monitoring, and Analysis of Audit Logs	In Place	90%	
CSC #7	Email and Web Browser Protections	In Place	90%	There's Symantec is used for Malware protection and updated as needed
CSC #8	Malware Defenses	In Place	90%	
CSC #9	Limitation and Control of Network Ports	In Place	80%	
CSC #10	Data Recovery Capabilities	Planned	0%	
CSC #11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	In Progress	60%	Policy has been revised. Information security will keep working with IT to ensure more secure configuration
CSC #12	Boundary Defense	In Place	80%	There's a good boundary protection mechanisms in place and Information security in putting ISAC malicious domain blocking in place
CSC #13	Data Protection	Planned	0%	
CSC #14	Controlled Access Based on the Need to Know	In Progress	50%	Data classification and governance policy revised awaiting approval
CSC #15	Wireless Access Control	In Place	90%	Wireless access to the authority users and guest are controlled and access points are monitored
CSC #16	Account Monitoring and Control	In Progress	50%	
CSC #17	Implement a Security Awareness and Training Program	In Progress	60%	Policy developed, training software procured, ongoing cyber awareness program and lunch and learn
CSC #18	Application Software Security	Planned	0%	
CSC #19	Incident Response and Management	In Progress	60%	Policy and program has been reviewed, and revised
CSC #20	Penetration Tests and Red Team Exercises	In Place	90%	Pen testing on train control systems and Red Team exercise conducted. Need to schedule for 2020 and 2012.