BOARD OF DIRECTORS

METROPOLITAN ATLANTA RAPID TRANSIT AUTHORITY

AUDIT COMMITTEE

THURSDAY, JULY 22, 2021

MARTA HEADQUARTERS

MEETING MINUTES

Committee Chair Freda Hardage called the meeting to order at 11:04 a.m.

Board Members Present	Staff Members Present
Roberta Abdul-Salaam	Jeffrey Parker
Stacy Blakely	Manjeet Ranu
William Floyd	Rhonda Allen
Freda Hardage, **Chair**	Melissa Mullinax
Al Pond	Elizabeth O'Neill
Kathryn Powers	Raj Srinath
Rita Scott	
Thomas Worthy	

Also in attendance: Board General Counsel Justice Leah Ward Sears of Smith, Gambrell & Russell, LLP, and other staff members: Emil Tzanov, Dean Mallis, Stephany Fisher, Kenya Hammond, Keri Lee, Tyrene Huff and Board Techs, Courtne Middlebrooks, Jonathan Brathwaite, Adrian Carter and Abebe Girmay.

Approval of the May 20, 2021 Audit Committee Meeting Minutes

Committee Chair Hardage called for a motion to approve the May 20, 2021 meeting minutes. Board Member Pond made a motion to approve, seconded by Board Member Worthy. The minutes were approved unanimously by a vote of 8 to 0 with 8 members present.

Resolution Authorizing the Solicitation of Proposals for the Procurement of External Audit Services for MARTA's Annual Financial Audits for Fiscal Years 2023 – 2027

Emil Tzanov, AGM Internal Audit, presented the above resolution for approval. On a motion by Board Member Pond, seconded by Board Member Floyd, the resolution was approved unanimously by a vote of 8 to 0.

- Board Member Pond suggested, it may be a good idea to have a fresh set of eyes for this particular contract. Mr. Tzanov gave a brief overview of the process on how proponents are selected and acknowledged the feedback from Board Member Pond. Board Member Abdul-Salaam asked about the DBE goal and Mr. Tzanov advised the goal is currently 20%. Board Member Floyd asked if there is a pre-approval process and Mr. Tzanov stated, the MARTA Act identifies several qualification requirements and proposals are reviewed based on those qualifications. Ms. O'Neill advised the Office of Contracts and Procurement will also send notices out to a variety of firms before issuing out the RFP.

Briefing – Internal Audit Activity *[Presentation attached]*
Emil Tzanov, AGM Internal Audit, presented a briefing on Internal Audit Activity.

- Board Member Floyd had questions about the roles of Audit and Cybersecurity. Board Member Hardage advised that a decision was made a while ago by the Board, that cybersecurity would fall under the Audit Committee. Mr. Parker advised on the roles, responsibilities, and lines of defense for both the Audit Department and Cybersecurity. Mr. Tzanov advised; we must be careful about governmental auditing standards as it relates to decision making. Board Member Pond asked about examples of the penetration tests where outside consultants try to get into our system and the corrective actions we have taken. Mr. Tzanov advised, Mr. Mallis and his team were the overseers of the penetration tests, but his team reviewed the reports and will follow-up with the corrective actions. Board Member Abdul-Salaam and Board Member Scott had additional questions about the risks and Mr. Tzanov addressed the questions.

Briefing – Information Security Update July 2021 *[Presentation attached]*
Dean Mallis, AGM of Information Security/CISO, presented a briefing on Cybersecurity.

- Board Member Floyd asked if there is anything the cybersecurity team is unable to complete due to a lack of funding. Mr. Mallis responded, no, he has received a lot of support from the Board, Mr. Parker and the CFO. Board Member Hardage asked how we fit in comparison to other transit agencies. Mr. Mallis advised we have a more mature program than most, but still have a long way to go. Mr. Parker asked Dean to speak about the meetings scheduled with other Chief Information Security Officers at various transit agencies to discuss best practices and policies. These meetings will take place very soon. Mr. Parker advised he is having discussions with APTA as well about cybersecurity. Board Member Hardage commended everyone for doing a great job.

Other Matters
None

Adjournment
The Committee meeting adjourned at 11:40 a.m.

Respectfully submitted,

Tyrene L. Huff
Assistant Secretary to the Board

YouTube link: https://youtu.be/pE8ZmiV0WD8

Internal Audit Activity Briefing

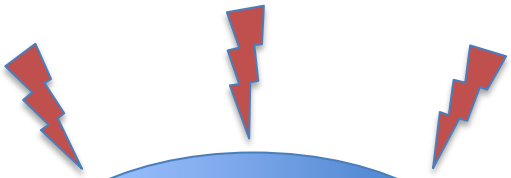
(04/01/2021 – 06/30/2021)

The Role of Internal Audit in Cybersecurity Assurance

Overall Oversight & Governance

Audit Committee

Executive Management



1st Line of Defense
Business Units and IT Function

2nd Line of Defense
Office of Information Security

3rd Line of Defense
Internal Audit

Roles & Responsibilities

- Execute cyber risk mitigation strategies
- Escalate risks outside of acceptable risk tolerance
- Embed Cyber in decision making

- Set policies and standards
- Select / help implement tools and processes
- Provide oversight, consultation and reporting

- Review program effectiveness
- Provide confirmation to the board of cyber risk management
- Verify regulatory compliance (future)

Internal Audit Cyber Assurance Strategy

the 3 Cs Approach

Competent

Victor Alade, CISA, CDPSE, CICA, GRCA, Certificate in Cybersecurity Fundamentals

Michael Oriade, CISA, CDPSE, Ph.D., Certificate in Cybersecurity Fundamentals

Comprehensive

- Anchor the Internal audit plan for cybersecurity on CIS (18) and NIST 800-53 frameworks
- Cover both the enterprise and the industrial control systems (train control and SCADA) environments
- Shift emphasis to “deep level” auditing (“the devil is in the details”)

Collaborative

- Continue collaboration and transparent communication with the Office of Information Security and the IT function
- Rigorously follow up on remediation of audit findings and other corrective action plans to help achieve improvement
- Benchmark and adopt best practices from other organizations

FY22 Information Technology Audit Plan *

Audit Name	Objective	MARTA Domain
Cybersecurity Insurance	Assess compliance with insurance policy requirements	Enterprise and Train Control/SCADA
Oracle Security	Evaluate application security and access to Oracle	Enterprise (Oracle only)
Password management	Assess password policies, controls, and configuration management	Enterprise (excl. Oracle)
Enterprise Pen-Test Remediation Follow-up	Review remediation of pen-test deficiencies	Enterprise
Train Controls System Pen-Test Remediation Follow-up	Review remediation of pen-test deficiencies	Train Control / SCADA
3rd Party Risk	Evaluate controls related to 3rd party IT risk	Enterprise

** The audits above are not listed in chronological order*

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
SOC1 Audit *	6/7/21	Low Risk	**Completed**	-	-	-	-	-	-	-	-
Property and Evidence Audit	6/7/21	Low Risk	**Completed**	-	-	-	-	-	-	-	-
Sales / Use Tax Financial Reporting Requirements (advisory)	6/7/21	Low Risk	**Completed**	-	-	-	-	-	-	-	-
Covid-19 Expenditures	6/30/21	Needs Attention	**Completed**	-	-	-	-	1	-	1	-
Total Significant & Moderate Findings:								1		1	

** "SOC" - System and Organization Controls Report*

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
Cubic-Automated Fare Collection System *	04/01/2021	Needs Attention	Completed	1	1		-	5	1	4	-
- Insufficient Monitoring of the Automated Fare Collection (AFC) System (6/30/2021)											
Direct Pay Process	10/31/2018	High Risk	Completed	3	2	-	1	-	-	-	-
- *Enhance and automate the External Training Request Form through Oracle. (7/1/19)*											
Capital Improvement Program – Follow-Up	1/15/21	Low	Completed	28	18	10	-	-	-	-	-
- *Expected implementation date extended to 8/3/21*											
Total Significant & Moderate Findings:				***32***	***21***	***10***	***1***	***5***	***1***	***4***	-

* *Integrated audit with the IT Audit Branch*

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 *	04/01/21	Needs Attention	**Completed**	1	1		-	5	1	4	-
- Insufficient Monitoring of the Automated Fare Collection (AFC) System (6/30/2021)											
Software Patch Management	06/30/21	TBD	**Draft Report**	-	-	-	-	-	-	-	-
CCTV Storage Capacity – Advisory	Q4	TBD	**Draft Report**	-	-	-	-	-	-	-	-
Total Significant & Moderate Findings:				1	1	-		5	1	4	

* *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
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. (05/31/21) - 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. (06/30/21)											
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) – Internal Audit confirming completion - Devices were running unsupported legacy software, which increases the risk of vulnerabilities being exploited. (5/31/20)											
Total Significant & Moderate Findings:				**11**	**5**	**4**	**2**	**4**	**1**	**1**	**2**

Contracts Audit Group

Audits Completed This Period (04/1/2021 – 6/30/2021)	
Audit Opinions	Audits Issued
Low Risk	13
Needs Attention	1
Total Audits Issued	14
Identified Unallowable Cost in Overhead Rate Reviews per Federal Acquisition Regulation ("FAR")	$357,416
Identified Potential Cost Savings in Cost/Price and Change Order Reviews	$69,039

Audits In Progress	
Audit Types	
Interim/Close Out	-
Rate Reviews	10
Cost/Price Analysis	2
Change Orders Special Audit (Incurred Cost, Special Request, Buy America & Claims)	3
Total Contract Audits in Progress	**15**

FY21 Audit Summary

Audits Completed in FY21	
Audit Branch / Type	**Audits Issued**
Contract audits	53
Identified Unallowable Cost in Overhead Rate Reviews per Federal Acquisition Regulation ("FAR")	*$1.6M*
Identified Potential Cost Savings in Cost/Price and Change Order Reviews	*$3.8M*
Performance Audit Engagements	7
Advisory Audit Engagements	10
Other (MARTOC)	1

Fraud, Waste, & Abuse (“FWA”) Summary

Eight calls received on the FWA hotline from April 1, 2021, to June 30, 2021

- 1 call alleging that a supervisor was sleeping on the job was referred to parking services. Internal Audit will perform a follow-up review.
- 1 call alleging that a customer was allowing a friend to use their Half-Fare Card was referred to Reduced Fare Eligibility Department. Internal Audit will perform a follow-up review.
- 1 call alleging that an employee was leaving the job early to go to their second job (outside of MARTA) was referred to Rail Car Maintenance. Internal Audit will perform a follow-up review.
- 1 call alleging that an employee was abusing FMLA by working a second job was referred to Human Recourses. Internal Audit will perform a follow-up review.
- 4 calls were forwarded to customer service for resolution.


marta
Bus
Stop
For Information Call 848-4711

Information Security Update July 2021

Audit Committee Meeting

marta

Information Security Update

Upcoming procurement initiates

Malicious Domain Blocking paid version

- 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.

CrowdStrike

- Advanced endpoint protection
- Threat hunting
- Proof of value completed.
- 85% of authority covered
- ~100% after the procurement

24/7 monitoring/vulnerability scanning vendor

Vendor will monitor network 24/7

Conduct vulnerability scanning

Save on FTE

Save on vulnerability scanner

Deployments

Multifactor Authentication (MFA) 99% complete.

- Forthcoming Requiring MFA for administrative role functions across the environment.

Antivirus replacement 85% complete

- CrowdStrike
- Windows Defender
- Layered Defense