



# CMPD Body-Worn Camera Program



**City of Charlotte**  
**Internal Audit Department**  
600 E. Fourth St.  
Charlotte, NC 28202

## **Staff**

### **City Auditor**

Tina Adams, CPA, CIA

### **Audit Supervisor**

Marie Marsicano

### **Senior Auditor**

Will Pellisero, CPA, CIA, CISA

To learn more about Internal Audit,  
please visit our [website](#).

**April 18, 2022**

# CMPD Body-Worn Camera Program Executive Summary

## Purpose

This audit was conducted to determine whether internal controls for CMPD's Body-Worn Camera (BWC) program are adequately designed, cameras were being used in accordance with state statute and department policy, and if the program meets the policy objective of promoting transparency and accountability.

## Background

A body-worn camera (BWC) is a small, battery-powered camera worn by police officers to record interactions with the public. The cameras are used to promote transparency and accountability through objective evidence. The policy includes procedures for: when to activate and deactivate the camera, when and where recording is prohibited, data retention, oversight, and the disclosure or release of videos. In FY 2021, officers uploaded 845,489 videos to Evidence.com. Since the BWC program's inception in 2015 through 2021, the City has paid Axon over \$12.5 million. These costs include BWC and TASER equipment, file storage, and training.

## Conclusion

CMPD has adequately designed controls for the BWC program, particularly ones ensuring critical events are recorded. Implementation of audit recommendations will help ensure the control system operates effectively and is adjusted as needed over time.

## Highlights

- CMPD's BWC policy is comprehensive and follows best practices.***  
Auditors compared CMPD's policy to industry best practices as well as peer cities, noting no material differences.
- Key controls exist to mitigate significant risks.***  
While auditors were unable to test the effectiveness of several controls due to limitations imposed by State law, the controls in place are well designed. CMPD has established key features to ensure BWC recordings of critical events are created and that reviews of those events happen.
- Periodic risk assessments are needed.***  
Assessing changes in risks ensures controls are adequately designed.

### ***Actions Planned:***

- CMPD will assess the adequacy of the monthly video sampling methodology, including the number of videos to be reviewed.
- Annually, Professional Standards Bureau (Professional Standards) will request Axon's SOC2 report and review it for any significant control deficiencies.
- Periodically, Professional Standards will review the Evidence.com Access Control List to ensure all users are assigned appropriate roles/permissions for accessing the BWC system. Following auditor inquiries, two users with elevated permissions had their roles corrected.

continued...

# CMPD Body-Worn Camera Program

## Executive Summary - continued

#### ***4. Existing monitoring controls need improvement.***

Due to State Statutes, auditors were not allowed to view BWC videos and therefore could not test the effectiveness of monthly division level reviews. CMPD should test the effectiveness of monthly division level reviews to reduce the risk of potential inconsistencies among supervisors. CMPD should also implement additional monitoring controls to ensure that calls for service are properly accounted for.

##### ***Actions Planned:***

- Bi-annually, Professional Standards will select a sample of supervisors' division-level reviews to check the adequacy and accuracy of review.
- CMPD will research establishing a process that ensures calls for service that should have a BWC video, in fact, have a video.

#### ***5. CMPD needs to consistently enforce the BWC policy.***

Consistent enforcement of the BWC policy can prevent minor policy violations. CMPD should reinforce the BWC policy requirements through additional training and ensure that supervisors are instructing officers to categorize and match videos at the end of each shift.

##### ***Actions Planned:***

- CMPD is currently revising the BWC directive to include language that refines the pre-shift equipment testing process. Test videos will be included during various division/unit inspections.
- Professional Standards will run a quarterly report identifying any undocked BWCs.
- Quarterly, Professional Standards will review and identify any video that has not been categorized, assigned a complaint number, or is an invalid test video and provide the list to the respective chain of command for follow-ups.

#### ***6. Opportunities exist to improve transparency and accountability.***

As the BWC program has grown, the use of in-car dash cameras (dash cams) has slowly been phased out. The equipment was obsolete, new equipment is expensive, and other options are becoming available. Public trust would be enhanced if the BWC program has a complementary technology that would allow recordings from various viewpoints. As technology evolves, CMPD is monitoring options to further promote transparency and accountability.

## Contents

Highlights .....	1
Objective.....	4
Background.....	4
Findings and Recommendations.....	10
1. <i>CMPD’s BWC policy is comprehensive and follows best practices.</i> .....	10
2. <i>Key controls exist to mitigate significant risks.</i> .....	10
3. <i>Periodic risk assessments are needed.</i> .....	11
A. <i>Monthly Review Sample Methodology</i> .....	11
B. <i>Third Party Service Providers</i> .....	12
C. <i>System Access Reviews</i> .....	13
4. <i>Existing monitoring controls need improvement.</i> .....	14
A. <i>Monthly Division-Level Reviews</i> .....	14
B. <i>Additional Monitoring</i> .....	16
5. <i>CMPD needs to consistently enforce the BWC policy.</i> .....	17
6. <i>Opportunities exist to improve transparency and accountability.</i> .....	20
Conclusion .....	22
Distribution of Report.....	22
Scope, Methodology, and Compliance.....	23
Appendix A .....	25
Appendix B.....	26
Appendix C.....	27

## Objective

---

As requested by the Chief of Police, this audit was conducted to determine whether:

- CMPD’s Body-Worn Camera program includes adequately designed internal controls
- Cameras were being used in accordance with state statute and department policy
- The program meets the policy objective of promoting transparency and accountability

## Background

---

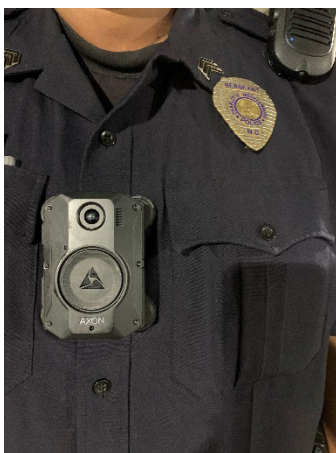
A body-worn camera (BWC) is a small, battery-powered camera worn by police officers to record interactions with the public. When powered on as required, BWCs have a 30-second buffering period. This always-on buffering allows 30 seconds of video to be recorded before BWC activation. Buffering does not capture audio.

CMPD’s BWC policy (Directive 400-006, available on [cmpd.org](http://cmpd.org)) states, in part, BWCs are used by officers to “promote transparency in accordance with state law and accountability for officers and the community through objective evidence.” Video recordings also provide objective evidence for officer performance reviews, aid in criminal investigations, and discourage inappropriate behavior by both CMPD officers and the public.



The policy includes procedures for: when to activate/deactivate the camera, when and where recording is prohibited, data retention, oversight, and the disclosure or release of BWC videos.

## Pre-Shift / Equipment Checks



The BWC is magnetically attached to an officer’s uniform. The proper center-chest placement is intended to best record activity within an officer’s field of vision (Exhibit A). The shift supervisors are responsible for ensuring all employees issued a BWC are properly wearing it prior to the start of their shift. Patrol officers and sergeants are issued two BWCs: one for on-duty and one as a backup (e.g., for secondary employment). Each camera is linked to its assigned officer’s unique ID (i.e., code number). Prior to each shift, sworn employees should ensure their BWC is on and all components are working.

Exhibit A: Proper BWC placement

## Activation & Deactivation

CMPD policy states, “BWCs shall be turned on and activated to record prior to arrival to any call for service or any crime related interaction with citizens while on duty or working secondary employment.” An officer can manually activate their BWC by pressing the “Event” button on the front of the device (Exhibit B). Once activated, the camera captures both audio and video. The recording will also include the video from the 30 second buffering period. To stop recording, an officer must press the button again.

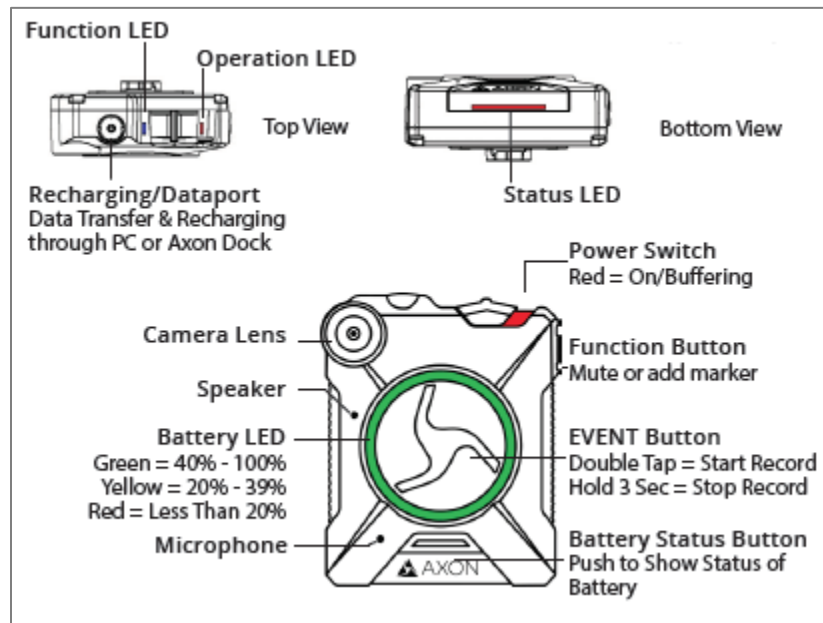


Exhibit B: Axon Body 2 (graphic courtesy of Axon)

Per the BWC Program Administrator, camera batteries typically last 12 hours on a full charge and have a minimum recording time of 6 hours. In addition to being manually activated, a BWC automatically activates in the following situations:

- Activation of vehicle blue-lights
- Officer unholsters sidearm
- Officer turns on TASER
- An officer performs any of the three aforementioned signal triggers within a 100' (30m) radius of another officer

The policy also outlines the appropriate time to deactivate a BWC recording as well as the next steps: “When an incident has ended, the officer shall stop the BWC recording and enter the appropriate category and, when necessary, the incident complaint number.” Officers can use the Axon View application on a smartphone to categorize and add additional information to their video(s).



## Data Management

At the end of each shift, officers are required to dock their BWCs on a designated docking station (Exhibit C). This automatically uploads any data collected to Axon's cloud storage system, Evidence.com, and charges the device. In FY 2021, officers uploaded 845,489 videos to Evidence.com. BWC videos can't be altered or deleted by users. They can only be deleted by System Administrators. In accordance with state law, uploaded videos are only viewable by the user/officer linked to that specific BWC, supervisors, and BWC administrators. As part of their responsibilities, certain units also have access to review BWC videos (i.e., Internal Affairs, Professional Standards, and the Independent Chain of Command Review Board).



Exhibit C: An Axon BWC docking station at CMPD's University Division

Officers must also properly categorize each video. The retention time of each video is based on these categories. Evidence.com maintains an audit trail for each video which tracks the date and time of each person who accesses it, as well as any changes made to the file's metadata<sup>1</sup>. Additionally, video metadata remains even after the footage is deleted.

## Oversight & Accountability

To aid in its objective of accountability, CMPD has several controls in place to monitor officer behavior; the review of BWC videos is one such control. Videos can be reviewed based on category/event-type or they can be selected randomly.

---

<sup>1</sup> a set of data that describes and gives information about other data

1. **MONTHLY REVIEWS** – the Crime Analysis division generates a stratified random sample of BWC videos for supervisory review. Supervisors highlight (in)correct tactics and positive/negative behavior and identify opportunities for improvement. These reviews are broken into tiers and documented in the BWC Audit Database.
  - Tier 1 – Supervisors review a sample of the month’s entire video population. Supervisors can also review video during their regular duties separate from the Tier 1 monthly reviews, as needed.
    - Every officer has at least one BWC video reviewed per month and more if they have any that fall into Tier 2 or are part of a “critical incident” i.e., an Officer-Involved Shooting (OIS)
    - Videos of critical incidents are reviewed separate from the monthly reviews
  - Tier 2 – Officers in the Professional Standards Bureau (PSB), a division within CMPD, review an additional sample of each month’s videos.
    - This sample includes videos associated with:
      - Felony cases accepted for prosecution
      - Discretionary arrests (e.g., “intoxicated and disruptive”)
      - Consent to searches during traffic stops or resident contacts
      - Officers in the top 5% of CMPD’s EIS<sup>2</sup> ranking
    - The PSB is also responsible for responding to all OIS incidents or other significant officer-involved incidents. The PSB representative will ensure all BWC footage related to the incident is downloaded as soon as possible and prepared for review by the Internal Affairs Bureau and the Police Chief. These OIS video reviews are separate from the Tier 2 reviews.
2. **TREND REPORTS** – Every month, the PSB gathers all the data from the above reviews, analyzes the results from the prior three months, and creates a report outlining trends. This “Monthly Trend Report” contains various statistics from the monthly random reviews, including: the number of videos reviewed, the percent of total videos reviewed, total viewing hours, etc. The report lists the number of “concerns” noted during the monthly BWC reviews by division, and includes information like the percent of concerns relative to videos reviewed, any repeat offenders, concerns by category, etc.
3. **COMPLAINT PROCESS** (Appendix A) – A “complaint” is an allegation that an officer broke one of 42 rules of conduct. Complaints can be generated by anyone (i.e., a fellow officer or a resident) and includes car crashes, raids & searches, officer injuries, discharge of firearms, vehicle pursuits, excessive force, etc.
  - **Internal Affairs** – conducts investigations when it’s determined a complaint needs to be reviewed. Every use-of-force event is required to be reported in the Internal Affairs Case Management System (IACMS) and its associated videos are reviewed by the

---

<sup>2</sup> Early Intervention System – System that employs predictive analytics and machine learning to better identify employees who may need assistance to improve interactions or behaviors (Directive 800-010)



investigating supervisor. Internal Affairs also reviews videos from other high-liability situations (e.g., pursuits, searches, etc.).

- **Independent Chain of Command Review Board** – this group is made up of supervisors and their peers who are not in an officer’s immediate chain of command. This group is convened to review certain Internal Affairs investigations.

## Disclosure, Release, & Transparency

BWC recordings are not public records and shall be disclosed only as legally allowed (N.C.G.S. 132-1). The law defines two different ways the public can view video(s):

1. Disclosure – “To make a recording available for viewing or listening to...”
2. Release – “To provide a copy of a recording.”

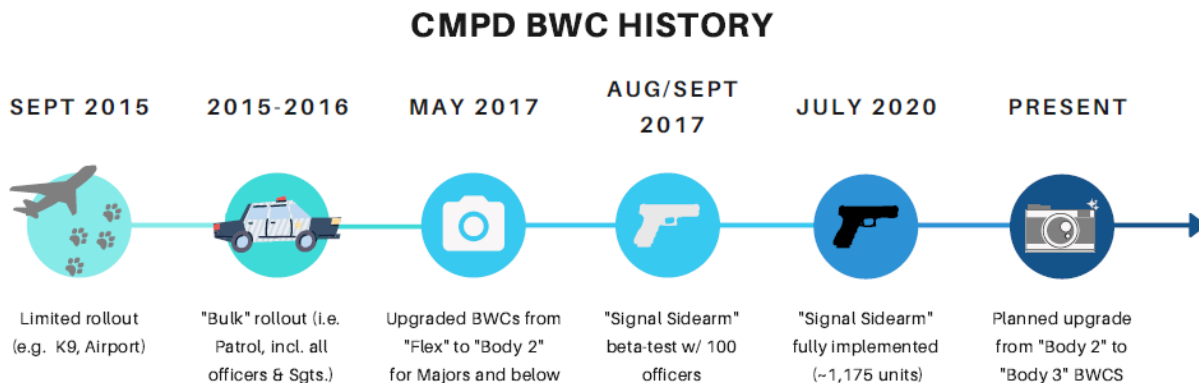
CMPD’s Professional Standards Bureau (PSB) handles disclosures. Per policy, “A person requesting disclosure of a recording must complete a Video Disclosure Request form located on the CMPD website.”

By law, disclosure requests must be made by someone in the video, the parent of a minor who is in the video, or a personal representative of someone in the video. The policy requires the CMPD BWC Administrator to contact the requesting party within five days of the disclosure request and, if approved, schedule a viewing time.

The City Attorney’s Office is responsible for coordinating with the Court system regarding the release of videos. The required form, Petition for Release of Custodial Law Enforcement Agency Recording (AOC-CV-270), is available at NCcourts.gov. Ultimately, the assigned Superior Court Judge must approve any release and the timing of video release(s) is dependent upon the Court system (Appendix B).

## Contract/Vendor History & Program Costs

Since the BWC program’s inception, Axon Enterprises (formerly TASER) has been the sole BWC supplier for CMPD.



The City has paid Axon over \$12.5 million since the CMPD BWC program’s inception in 2015 through 2021 (Figure 1). These costs include BWC and TASER equipment, file storage, and training. The City also participates in the TASER Assurance Plan which provides a warranty, unlimited BWC video storage, and camera and dock replacement every 2-½ years. Most of the 2017 expenses were for a “TASER refresh” (\$3M).

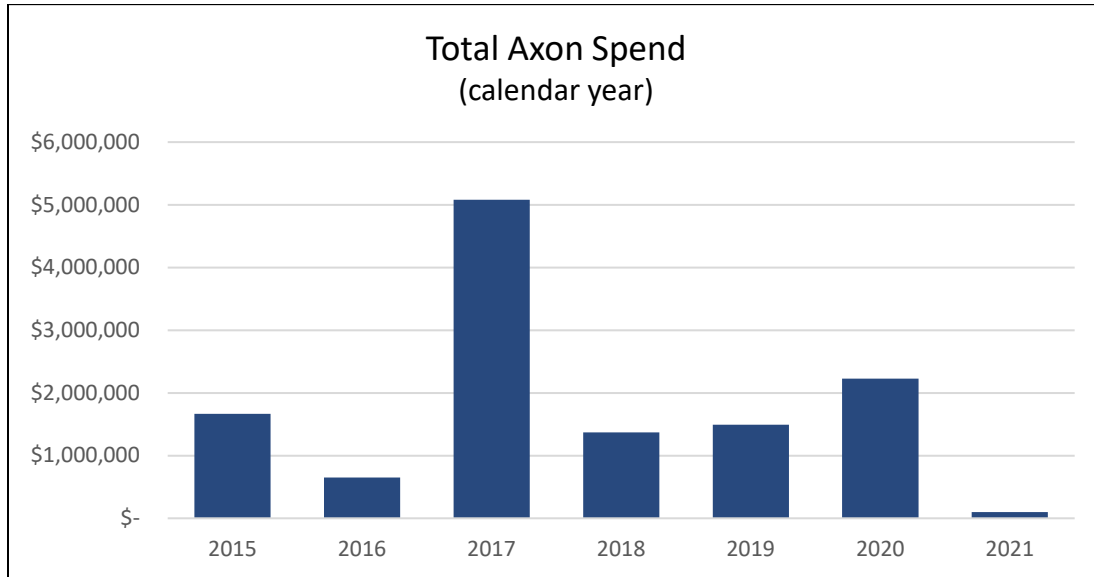


Figure 1: Payments to Axon, by calendar year

## Findings and Recommendations

Body-worn cameras (BWCs) are only effective in increasing officer accountability if well-designed controls are in place and functioning effectively. While auditors were unable to test the effectiveness of several controls due to limitations imposed by State law, the controls in place are well designed.

### 1. *CMPD’s BWC policy is comprehensive and follows best practices.*

In addition to comparing CMPD’s BWC policy to industry best practices, auditors also compared it to the policies of six peer cities and found only minor differences. Regarding the two best practices CMPD’s policy is missing, four of the six peer cities had guidance on informing the public of recording and only one addressed the use of biometrics.

Policy Element	CMPD	CALEA	IACP	BJA	COPS	BWC scorecard	ACLU
Purpose	✓	•	•				
Policy Statement	✓	•	•				
Recording requirements & restrictions	✓	•	•	•	•	•	•
Guidance on informing public of recording	✗		•		•	•	•
Video upload & categorizing/tagging deadlines	✓		•		•		
Restrictions on editing, distribution, or other uses	✓	•	•	•	•	•	•
Storage & retention	✓	•	•	•	•	•	•
Public release process	✓		•	•	•	•	
Requirements for supervisors	✓	•			•		
Formal policies for video reviews	✓	•	•	•	•	•	
Policy available to public	✓			•	•	•	
Addresses use of biometrics (i.e., facial recognition)	✗					•	

Figure 2: CMPD’s BWC policy compared to industry best practices

### 2. *Key controls exist to mitigate significant risks.*

As detailed in the Background section, numerous procedures are in place to reduce the risk a critical event or unprofessional officer behavior is not recorded.

The various BWC auto-activation features are an effective way for CMPD to ensure critical events are recorded. This is especially important for officer-involved shootings (OIS) where the Signal Sidearm feature ensures an officer’s BWC is recording in the event they unholster their service weapon. BWC footage serves as an important piece of evidence for OIS (Appendix C), but also other high-liability events such as TASER deployments and high-priority calls-for-service – both of which are covered by BWC auto-activation features (i.e., TASER-

power-on and police cruiser blue light activation). These are effective preventative controls ensuring BWC footage exists for critical events.

Evidence.com allows for users to be grouped into various access levels based on position-needs. The system also keeps a detailed audit trail that logs any access or changes made to individual BWC files. CMPD has a variety of monitoring controls in place, mainly via system reports and monthly random video reviews.

Monitoring exists as a detective control to hold officers accountable for unprofessional behavior. This monitoring also ensures officers use correct tactics, can highlight positive behaviors, and identifies opportunities for improvement. The Tier 1 and Tier 2 monthly reviews (as outlined in the Background section) ensure every officer has at least one video per month reviewed.

### 3. Periodic risk assessments are needed.

CMPD has key features in place to ensure BWC recordings of critical events are created and that reviews of those events happen. Like any evolving program, there are opportunities for CMPD to improve the administration of the BWC program.

The COSO internal control component “Risk Assessment” includes the principle “Identify and analyze significant change.” Periodically assessing changes in risks ensures controls are adequately designed.

#### A. Monthly Review Sample Methodology

Monthly, supervisors review at least one video for each officer. Since the CMPD BWC program’s inception, no analysis has been performed to confirm the methodology is still producing an adequate number of sampled videos for review.

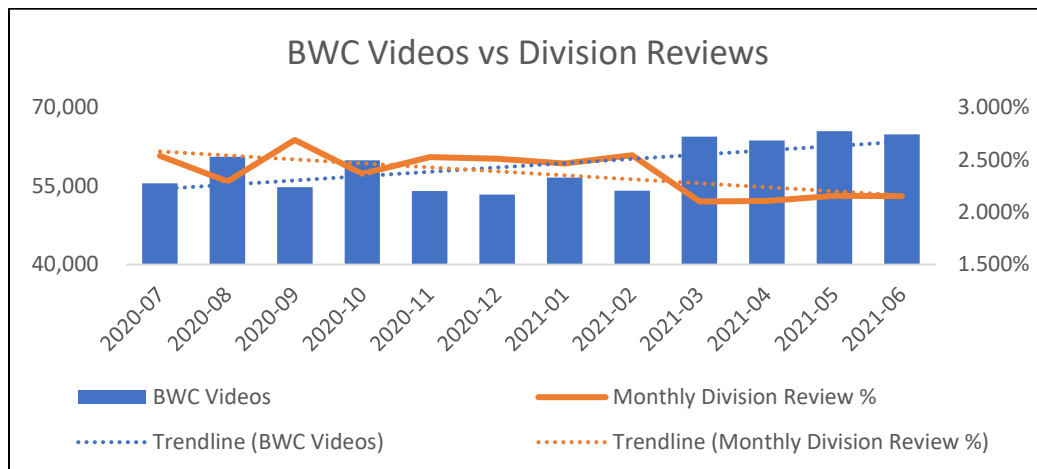


Figure 3: Percent of BWC videos reviewed during each month’s Division Tier-1 reviews

As Figure 3 shows, calls-for-service and the resulting number of monthly BWC recordings are increasing. Since the sample is a static number of videos, the percentage of videos reviewed will continue to decrease. This lessens the monthly division-level/Tier 1 random reviews' impact on officer accountability. The same issue affects Tier 2 reviews. This is most evident in the "Consent-to-Search" category (Figure 4).

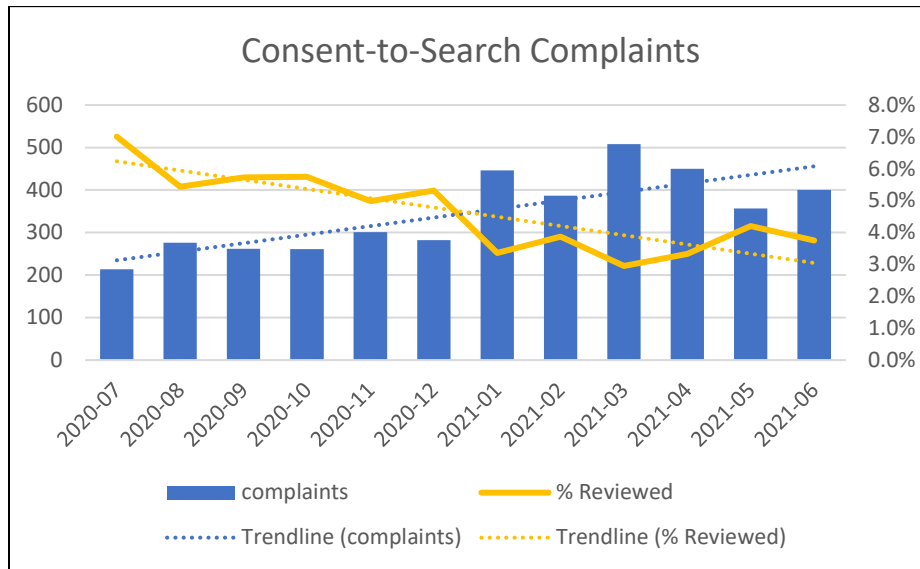


Figure 4: Percent of Consent-to-Search complaints reviewed over time

**Recommendation:** CMPD should assess the adequacy of the monthly video sampling methodology, including the number of videos to be reviewed. A reassessment should be performed annually. If/when changes are made to the methodology or system, the reassessment should occur after enough time has passed to allow for any recent changes to take effect.

**Value Added:** Risk Reduction

**CMPD Response:** CMPD agrees. A documented assessment of the current monthly video sampling method will be generated by Professional Standards by March 31, 2022. Any recommended changes will be tested for suitability and negative impacts by May 31, 2022, and if deemed suitable and have minimum risks, will be implemented by June 30, 2022. Re-assessment of the video sampling methodology will be performed by Professional Standards every 3 years to ensure no programming defects; compatibility with accompanying systems; adequate amount of data to achieve changed requirements; and feedback from users.

## B. Third Party Service Providers

Data management and system controls over BWC data are critical to a well-functioning BWC program. Axon/Evidence.com plays an integral role in the management of BWC-video evidence. These videos are also used as part of the documentation of officer performance issues (good and bad). Because of its importance and the confidentiality of the underlying

data, Axon's internal controls (as the third-party service provider) and CMPD securing access to the Evidence.com system are critical.

Service organizations often use Service Organization Controls (SOC) reports to build trust and confidence in their systems to other entities. SOC2 reports contain detailed information relevant to system security, availability, and processing integrity. Due to the confidentiality of this information, these reports are often restricted.

Axon receives a SOC2 report annually. Auditors reviewed the 2020 report, noting no significant incidents resulting from inadequate controls. However, CMPD has not been requesting this report. Without reviewing Axon's SOC2 report, CMPD could be unaware of Axon-related control issues that may negatively impact department operations. Annually reviewing this report would provide CMPD insight into Axon's control environment.

**Recommendation:** CMPD should annually request Axon's SOC2 report and review it for any significant control deficiencies.

**Value Added:** Risk Reduction

**CMPD Response:** CMPD agrees to annually request Axon's SOC2 report and to review it for any significant control deficiencies that could negatively impact CMPD operations. CMPD will request the 2021 report by March 31, 2022.

### C. System Access Reviews

Evidence.com functions are accessed based on user roles. The standard role limits access to viewing only videos recorded on that officer's assigned BWC. Video that has been specifically shared by authorized users can also be viewed by a standard user. Supervisors can view all non-restricted data as they are responsible for ensuring officer compliance with CMPD policies. System Administrators have full access to the system; this role is limited to only 14 CMPD staff.

A comparison of the Evidence.com user access control list and the CMPD active roster showed two users (of 1,930) had unnecessary permissions. Per CMPD, these were users that had an appropriate level of access, retired, were rehired in different roles, and given their old access level. Additionally, this test's exceptions are relatively minor due to other mitigating controls in place:

1. Microsoft Active Directory – The system requires the user accounts be active in both CMPD's Active Directory (AD) and Evidence.com. Once an account is deactivated in AD, they no longer have access, regardless of their Evidence.com account status.
  - a. System access is also only granted while users are on the City's secure network
2. Weekly HR Announcements – changes in employment status are communicated weekly from HR. User changes are made as needed from this announcement.



3. BWC Equipment Return(s) – when an officer returns their equipment (i.e., retirement, resignation, termination), system access is changed.

Best practice is to also have a periodic access control review process in place; CMPD had no such procedures established at the time of the audit.

**Recommendation:** CMPD should periodically review the Evidence.com Access Control List to ensure all users are assigned appropriate roles/permissions for accessing the BWC system.

**Value Added:** Risk Reduction

**Actions Taken:** Following auditor inquiries, the two users with elevated permissions have had their roles corrected. The first review was conducted on 10/01/2021.

**CMPD Response:** CMPD agrees. Quarterly, Professional Standards will:

1. Review the Evidence.com access control list to ensure all users are assigned appropriate roles/permissions, and
2. Implement any necessary changes, including but not limited to updating individual roles/permissions, updating permissions to roles, etc.

#### **4. Existing monitoring controls need improvement.**

CMPD's BWC program is based on a comprehensive policy and there are adequate controls in place for it to meet its objectives. However, given that BWC technology is constantly evolving, there are opportunities for improvement. This is especially true regarding various monitoring controls in use by supervisors and the Professional Standards Bureau (PSB).

The COSO internal control component "Monitoring Activities" has two relevant principles:

1. Conducting ongoing and/or separate evaluations
2. Evaluating and communicating deficiencies

##### **A. Monthly Division-Level Reviews**

The monthly random review of BWC videos is designed to promote officer accountability by ensuring that each officer has, at a minimum, one video reviewed per month. Any policy violations or opportunities for improvement are noted on the BWC Audit Form as a "concern."

Auditors analyzed monthly review data for FY21. Some supervisors completed a high number of reviews yet did not document a single concern. Specifically, 24 supervisors viewed between 50-170 videos each (totaling 2,216 videos) and found no concerns. While not all reviews will result in a concern, the average FY21 "Concern Percentage" is about 3% per reviewer. Given the scope of what supervisors look for during their monthly reviews, it is

unlikely that the 2,216 videos viewed yielded no concerns. Currently, CMPD is not analyzing supervisors' BWC review performance.

Proper testing of the effectiveness of this control, reduces the risk that a reviewer is completing the form but not actually performing the review. Periodically checking reviewer performance (i.e., the reviewer has adequately and accurately completed the monthly video reviews and the BWC Audit Form), ensures that the monthly reviews are having the desired impact of improving officer behavior and/or holding officers accountable for poor conduct.

The adequacy of supervisor reviews also impacts another monitoring control: the "Monthly Trend Analysis" report. This report is distributed to CMPD Leadership and shows statistical trends as detailed in this report's Background section. Based on a review of the FY21 monthly trend reports and other details provided by PSB, it is evident the report is in use and is an adequately designed monitoring control. However, this report is only as good as the underlying data – the monthly supervisor reviews. Without the ability to view a sample of reviewed videos to verify supervisor comments (or lack thereof), auditors were not able to assess the effectiveness of this control.

**Recommendation:** The PSB should randomly select a sample of supervisors' division-level reviews each month to check the adequacy and accuracy of review. As an alternative, the PSB should ensure someone in a supervisor's chain of command is periodically reviewing their staffs' monthly reviews, on a sample basis.

**Value Added:** Risk Reduction; Compliance

**CMPD Response:** CMPD Agrees. On a bi-annual basis, PSB will:

1. Identify supervisors who have consecutively noted no concerns for all videos reviewed in the past 6 months.
2. For each identified supervisor, a random selection of videos that have yet to be deleted will be reviewed to check the adequacy and accuracy of review.

## B. Additional Monitoring

One of the key requirements of the policy is that BWCs should be activated “prior to arrival to any call for service or any crime related interaction with residents while on duty or working secondary employment...” The three relevant COSO internal control principles (and the associated component) are:

- Enforces accountability (Control Environment)
- Deploys control activities through policies and procedures (Control Activities)
- Conducts ongoing and/or separate evaluations (Monitoring Activities)

CMPD could implement additional monitoring controls to ensure officers are activating their BWCs before arriving to any call for service by incorporating the use of computer-aided dispatch (CAD) information into its existing monitoring activities.

For FY21, Auditors analyzed CAD data for Priority 0-1 calls<sup>3</sup> and noted 34% of these calls did not have a corresponding BWC file.

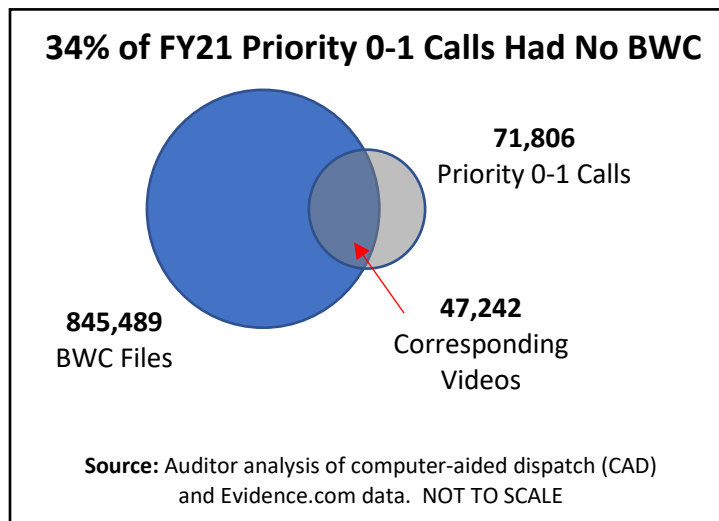


Figure 5: Priority 0-1 calls (from CAD) matched to BWC data

Per CMPD, the 34% of Priority 0-1 calls with no corresponding BWC file could be due to several factors:

- Axon/Evidence.com may have auto-tagged a file incorrectly
- A complaint number could be a duplicate
- BWC not required (e.g., responding to a call where medical aid is being given)
- Calls cancelled before an officer’s arrival (or that did not require police)

<sup>3</sup> Based on Priority Code Description, these were assumed to be the calls-for-service most likely to have an officer responding w/ their blue lights on (i.e., they should have an automatic-BWC activation)

Priority 0 = Officer requests assistance, Officer in Trouble

Priority 1 = Emergency Priority-Life Threatening, in Progress, Suspect on Scene

Analysis of the detailed call categories that make up the 34% of Priority 0-1 calls shows the majority (70%, see Figure 6) are likely valid exceptions based on section IV.F.31 of the policy:

*"To aid in the protection of the right to privacy, sworn employees shall not record while: a. In a patient care area of a health care facility, unless the patient becomes adversarial with the officer or others..."*

Based on a small judgmental sample of calls within each category below, dispatch notes for many indicate the call was either cancelled before a CMPD officer arrived or medical aid was in process when CMPD arrived.

Description	# w/ no BWC	% of Total
ASSIST MEDIC	5,915	24.1%
ACCIDENT-PERSONAL INJURY	5,602	22.8%
CHECK THE WELFARE OF	1,970	8.0%
ASSIST FIRE DEPARTMENT	1,943	7.9%
SUICIDE-THREAT	777	3.2%
ADW- WITH INJURY	517	2.1%
OVERDOSE	490	2.0%
	<b>17,214</b>	<b>70.1%</b>

Figure 6: Medical-related call categories

It is not clear what percentage of calls should have video available.

**Recommendation:** CMPD should establish a process that ensures calls for service that should have a BWC video, in fact, have a video.

**Value Added:** Risk Reduction; Compliance

**CMPD Response:** CMPD Agrees. CMPD will:

1. Consult with Axon as to whether a process to ensure calls for service that should have a BWC video, in fact, have a video can be established.
2. Contact other police departments to inquire as to whether they have a process to ensure calls for service that should have a BWC video, in fact, have a video.
3. Evaluate all information gathered and implement, if any, process to ensure calls for service that should have a BWC video, in fact, have a video.

## 5. **CMPD needs to consistently enforce the BWC policy.**

Controls are adequately designed, and the recommendations above would strengthen CMPD's administration of the BWC program. However, without adequate and consistent enforcement, policy violations are occurring. These violations are the result of pre-shift and end-of-shift controls not operating effectively.

### Pre-Shift Equipment Tests

Policy requires a pre-shift test of all available BWC auto-activation devices. Through interviews, analysis of department-wide patrol schedules, and a sample of detailed officer BWC data, officers were not consistently testing each feature of the BWC system. Auditors randomly sampled 40 officers with June 2021 BWC recordings. Ten of the 40 (25%) were missing a BWC video categorized as “test.” Furthermore, most of these 30 officers with a test video had just one daily test video (versus the three required by policy). Inadequate pre-shift tests of the BWC equipment could result in an officer being on patrol with malfunctioning equipment.

### BWC Docking

Officers are required to dock their BWCs immediately following their shift. Prompt docking ensures BWC files are backed up and secured within Evidence.com. Three of the 40 (8%) officers sampled had audit trails indicating their BWCs were not docked at the end of their shift.

Additional analysis of the full FY21 BWC video population shows the majority of BWC videos (94.4%) are uploaded within three days of recording: the amount of time allotted to officers working secondary employment (and the longest recording-to-docking time allowed). However, Figure 7 shows that 5.6% of videos were not uploaded within three days of recording. Excess delays in BWC docking could result in some videos not being subject to review.

Days to Upload	BWC Count	Percent of Total	
0	489,169	57.9%	
1	274,901	32.5%	
2	20,632	2.4%	
3	13,441	1.6%	94.4%
4 to 7	32,450	3.8%	
8 to 14	9,184	1.1%	
15 to 30	4,053	0.5%	
31 to 364	1,644	0.2%	
> 365	15	0.0%	5.6%
<b>Grand Total</b>	<b>845,489</b>		

Figure 7: Days elapsed from recording to docking/upload

### Video Categorizing

Officers are required to categorize all of their BWC recordings prior to the completion of their shift. This can be completed after docking the BWC or during the officer’s shift via the Axon View app. Auditors reviewed documentation for each of the 40 randomly sampled June 2021

BWC recordings; four (10%) were not categorized timely. The delay ranged from four to 14 days.

It's important to note, this was a small, non-statistical sample and can't be extrapolated to the entire population. Additionally, CMPD has monitoring controls – in the form of system reports – to identify uncategorized videos and videos with no complaint number.

Reports are available as needed to command staff and a weekly general summary is provided to supervisors. The reports are well designed; however, they are not being used effectively. The June 28, 2021 reports, for example, showed numerous BWC videos with policy violations: either they were uncategorized or had no assigned complaint number.

Additional analysis of the BWC video population showed that of the more than 845,000 BWC videos recorded in FY21, there were:

- 1,759 uncategorized videos resulting in a total uncategorized error rate of approximately 0.21%. Of these, 671 were uncategorized for more than 1 week.
- 1,137 videos with no matching complaint number resulting in an error rate of approximately 0.13%. Of these, 678 were unmatched for more than 1 week.

Categorizing videos is critical because each video's category determines the video's retention time. On the 6/28/21 report, no uncategorized videos were nearing the 1-year deletion date, but the risk exists that a video is uncategorized and could be deleted based on Evidence.com retention settings. Videos without an assigned complaint number also violate policy.

In most cases, officers are following the policy. However, even a small percentage of noncompliance (0.21% and 0.13%) results in thousands of entries on the reports. The reports' purpose is to highlight individual files not meeting policy requirements. With such a high quantity of aged files populating each report (detailed above), the reports are less useful in identifying new files that are policy exceptions. If the reports are not used to remediate policy violations, BWC evidence could be difficult to locate or lost.

**Recommendation:** CMPD should reinforce the BWC policy requirements through additional training. Supervisors should ensure officers are categorizing and matching videos at the end of each shift. Performance should be monitored by command staff and disciplinary action taken for repeat non-compliance.

**Value Added:** Risk Reduction; Compliance

#### **Actions Planned:**

##### **Pre-Shift Equipment Tests**

1. CMPD is currently revising the BWC directive to include language that refines the pre-shift equipment testing process.



2. Professional Standards took the following corrective actions:
  - a. During various inspections, the inspected division/unit is provided a list identifying every individual in their division/unit and their number of BWC videos and number of TEST videos for the past 3 months.
  - b. For individuals chosen for the monthly EIS-BWC reviews, the number of BWC videos including TEST videos are provided to PSB supervisors to follow-up with the officers' chain(s) of command, if necessary.

### **Docking**

Professional Standards will, on a quarterly basis, run a report identifying the docking status of BWCs. The list of BWCs that have not been docked will be sent to the individual and their chain of command for corrective action.

### **Video Categorizing and Complaint Number Assignment**

1. The OnDemand Reports and Compliance Dashboard will continue to be used. The majority of the divisions/units do use the tools and ensure that videos are categorized and are assigned a correct complaint number in a timely fashion.
2. Professional Standards will continue to provide divisions/units with their average BWC errors (uncategorized videos, invalid test, no/invalid complaint number) statistics during various inspections.
3. Professional Standards will emphasize the need to categorize and assign the corresponding complaint number to their videos during the prescribed timeframe during officer and Sergeant trainings.

Quarterly, Professional Standards will review and identify any video that has not been categorized, assigned a complaint number, or is an invalid test video and provide the list to the respective chain of command for follow-ups.

**CMPD Response:** CMPD agrees and will continue to perform the corrective actions as outlined above and ensure that controls are functioning as intended.

## **6. Opportunities exist to improve transparency and accountability.**

CMPD places great emphasis on being a proactive partner with the community they serve and the importance of trust and accountability. It's part of the CMPD Mission Statement:

*"CMPD implements solutions and expands collaborative relationships within our organization and community to enhance trust, fairness and respect, to increase public safety."*

It's also emphasized in the BWC policy which states the purpose of BWCs is to promote transparency and accountability.

As the BWC program has grown, the use of in-car dash cameras (dash cams) has slowly been phased out. The equipment was obsolete, new equipment is expensive, and other options

are becoming available. Public trust would be enhanced if the BWC program has a complementary technology that would allow recordings from various viewpoints. As technology evolves, CMPD is monitoring options to further promote transparency and accountability.

Additionally, police departments’ internal investigations across the U.S. are regularly criticized for the perceived lack of independence. While the public’s trust would be better earned through a review process independent of CMPD, the strict State statute severely limits who can and cannot view BWC videos. External reviews would increase the legitimacy of any monitoring controls and program oversight.

CMPD has several avenues for investigating an officer accused of misconduct, which includes the viewing of any available BWC footage [Appendix A]. Per CMPD Internal Affairs’ 2020 Annual Report, 95% of the 114 total allegations were sustained (i.e., “The investigation disclosed sufficient evidence to prove the allegation made in the complaint”). Most complaints are generated internally within CMPD (72%) and are often the result of the monthly BWC random reviews and other supervisory video reviews.

As shown in Figure 8, this is also true for the specific complaint category “Use of Body Worn Camera.”

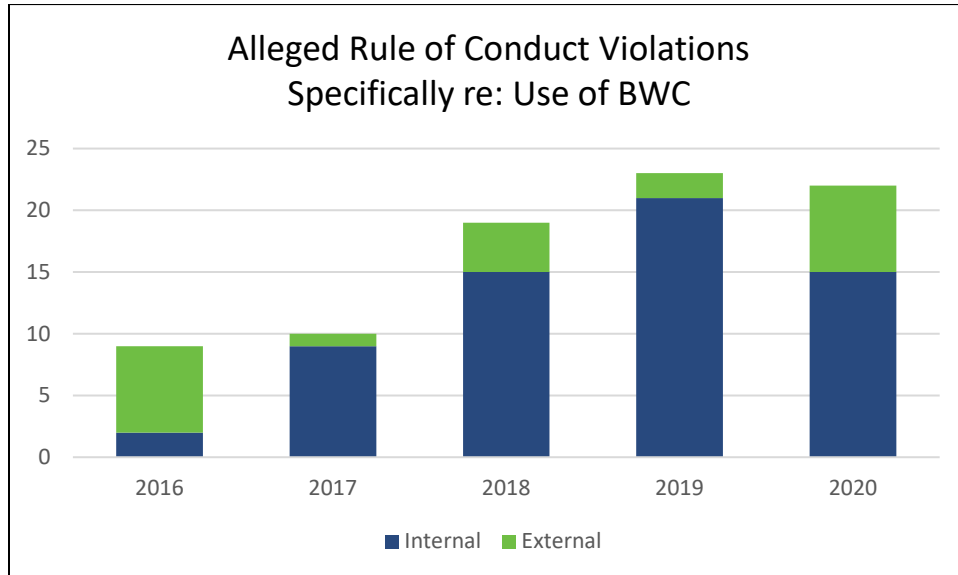


Figure 8: Alleged BWC-related Rule of Conduct Violations

Where they can, CMPD should continue to explore opportunities to enhance transparency and accountability.

## Conclusion

---

CMPD has adequately designed controls for the BWC program, particularly ones ensuring critical events are recorded. Implementation of audit recommendations will help ensure the control system operates effectively and is adjusted as needed over time.

## Distribution of Report

---

This report is intended for the use of the City Manager's Office, City Council, and CMPD. Following issuance, audit reports are sent to City Council via the Council Memo and subsequently posted to the [Internal Audit website](#).

## Scope, Methodology, and Compliance

---

### Scope

This audit reviewed BWC program performance and video metadata for FY2021. Auditors tested the design of internal controls. Due to a state statute preventing outside parties from viewing BWC footage, auditors were unable to test the effectiveness of several controls. The scope included: CMPD policies on BWC, CMPD training materials, hardware and software used by CMPD, and data generated during BWC program use.

### Methodology

To achieve the audit objectives, auditors performed the following:

- Interviewed CMPD management and staff, CMPD Professional Standards Bureau staff, CMPD Crime Analysis Division staff, and a CMPD Attorney
- Compared CMPD BWC policy to the following standards/best practices:
  - CALEA Standard 41.3.8 – “In-car and/or Body-Worn Audio/Video”
  - International Association of Chiefs of Police Body-Worn Cameras “Considerations Document” (April 2019) and “Concept & Issues Paper” (July 2019)
  - U.S. DOJ Bureau of Justice Assistance “Body-Worn Camera Toolkit Implementation Checklist” (2015)
  - U.S. DOJ Community Oriented Policing Services and the Police Executive Research Forum “Implementing a Body-Worn Camera Program Recommendations and Lessons Learned” (2014)
  - The Leadership Conference on Civil and Human Rights and Upturn’s “BWC Scorecard” (November 2017)
  - The ACLU’s “A Model Act for Regulating the Use of Wearable Body Cameras by Law Enforcement”
- Benchmarked/Surveyed BWC policies and monitoring procedures with peer departments in NC and across US
- Analyzed Evidence.com video metadata for FY2021, including data related to:
  - Unclassified and/or untagged videos
  - The timing of video upload and categorization
- Reviewed system logs for indication/frequency of supervisor review
- Compared BWC system data with CAD (computer-aided dispatch) activity
- Compared BWC system data with officers’ work schedules
- Randomly sampled and examined Evidence.com audit trail logs
- Evaluated fraud-related risks associated with officer use of BWCs and CMPD’s storage and retention of BWC video(s)
- Reviewed State law related to BWCs and the public release/disclosure of BWC video(s)
  - Randomly sampled BWC video disclosure requests and release petitions looking specifically for completed documentation and timely video review

- Reviewed Axon Enterprise, Inc.'s Service Organization Controls (SOC2) report for identified control issues for the period 01/01/20 – 10/31/20
- Evaluated user permissions in Evidence.com and software access controls
- Analyzed Evidence.com system controls to determine whether videos were retained in accordance with retention guidelines and whether videos could be deleted by unauthorized users
- Visited three CMPD divisions and observed the various BWC auto-activation features

Data obtained was evaluated to ensure it was valid and reliable. As necessary, auditors selected samples of the data in a variety of ways (judgmentally, haphazardly, and randomly). There were no statistical samples made; therefore, test results from these samples are not intended to be extrapolated to the entire BWC population.

## Compliance

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

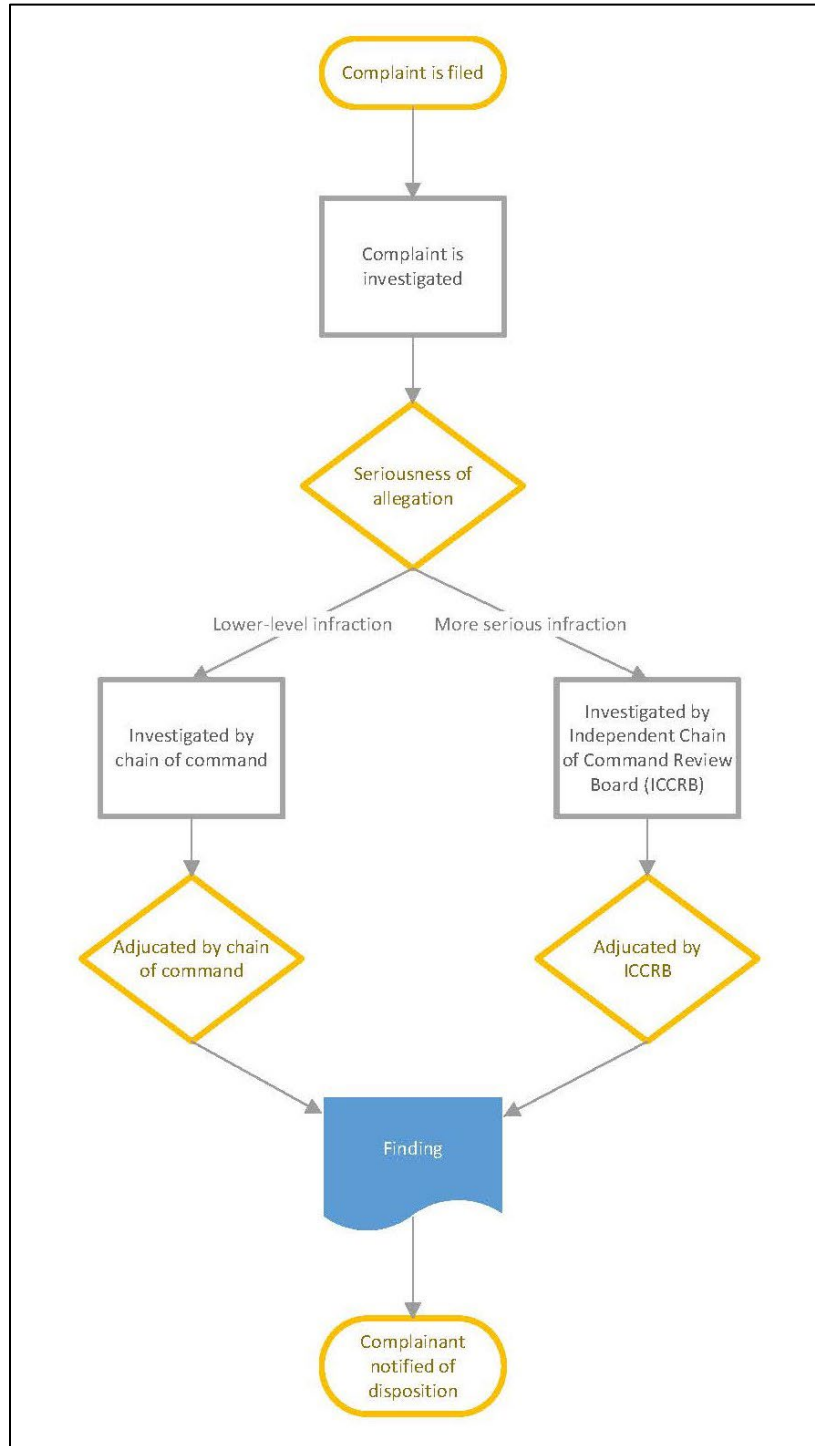
Government auditing standards require that we determine which internal controls are material to the audit objective(s) and obtain an understanding of those controls. To evaluate internal controls, the City Auditor's Office follows the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework (COSO Framework) as included in Standards for Internal Control in the Federal Government (GAO Green Book).

In planning and performing the audit, auditors obtained an understanding of the processes used throughout the BWC program and the associated internal controls, assessed the internal control risks, and determined the following internal control components were significant:

- **Control Environment** – The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization
- **Risk Assessment** – The process for identifying and assessing risks that may limit the achievement of objectives
- **Control Activities** – The actions management establishes through policies and procedures to achieve objectives and respond to risks
- **Information & Communication** – The quality of information which management and personnel communicate and use to support the internal control system
- **Monitoring** – The activities management uses to assess the quality of performance over time

Internal control deficiencies that are significant within the context of this audit's objective(s) are stated in the Findings and Recommendations section of this report.

## Appendix A



Source: Internal Audit Process Map



## Appendix B



Source: CMPD

## Appendix C

### CMPD OFFICER-INVOLVED SHOOTING INVESTIGATION PROCEDURE

PURSUIT OF JUSTICE - TRANSPARENCY - THOROUGHNESS - FACTUAL - ACCOUNTABLE



Shooting occurs, media briefing and social media messaging to share preliminary information with the community



Within 24 hours, Public Affairs shares updates, context, officer involved

#### TWO PARALLEL, INDEPENDENT INVESTIGATIONS

##### ADMINISTRATIVE

Internal Affairs Bureau launches internal investigation to determine whether the officer violated department policies and procedures



Officer placed on paid administrative leave and then administrative assignment



Independent Chain of Command Shooting Board (Community Relations Committee and High-Ranking CMPD Personnel) Hearing – Scheduled following DA decision



Evaluates officer's actions to determine if policies and procedures were followed

**YES**      **NO**



Officer re-instated to full duty status if policies and procedures were followed



If officer cited for suspension, demotion or termination, case is heard by the Civil Service Board

##### CRIMINAL

Officer-Involved Shooting Team conducts the criminal investigation



Interview witnesses



Gather information



Review evidence



\* Review the body worn camera video and audio

\* Body worn camera public release is determined by a superior court judge.

State Medical Examiner's Office



Leads investigation of the deceased



Conducts autopsy

Mecklenburg County District Attorney's Office



Conducts independent review and analysis of the Medical Examiner's Office findings



Determines if further investigation is needed

Whether criminal charges against the officer are appropriate

**YES**

**NO**



If felony charges are required, the case is presented to a grand jury to consider indictment



Clears officer of criminal charges by determining the shooting was justified

