# Public RLA Oversight Protocol

Stephanie Singer and Neal McBurnett, Free & Fair
Copyright Stephanie Singer and Neal McBurnett 2018
Version 1.0

One purpose of a Risk-Limiting Tabulation Audit is to improve public confidence in election outcomes (presuming the evidence supports such confidence). To this end, it is crucial that the public have confidence in the audit itself. One might wish for an audit process so simple that any voter could oversee and check it. The complexities of a Risk-Limiting Tabulation Audit may put its verification out of reach of some individual voters; however, if the agency conducting the audit makes certain information and processes available to the public, any individual or group with some quantitative tools and skills should be able to check the correctness of the audit.

For the Risk-Limiting Tabulating Audit to achieve its purpose,

- The agency conducting the audit must release sufficient information and open the processes of the audit up to careful public observation
- At least one (and preferably several) independent entities should observe and check the correctness of the audit.

The authors wish to thank Harvie Branscomb for his close reading and suggestions for improvement.

# Protocol to Check Correctness of Colorado's Risk-Limiting Tabulation Audit

To check the correctness of the Colorado risk-limiting tabulation audit, carry out the following steps. We believe these to be a minimum set of necessary items to verify that the evidence produced as part of the audit limits the risk of an incorrect tabulation outcome as intended and supports the audit's conclusions.

## Note on Scope

End-to-end verification of election results requires more than verification of the tabulation outcomes for the contests for which a specific risk limit is set. Other issues to include in any end-to-end election audit would include:

- Auditing the full chain of custody for ballots from when they are cast until election outcomes are finalized
- Translation of voter intent from sources other than a paper ballot card verified by a voter, such as electronically-implemented UOCAVA ballots (emails, faxes, and other forms of Internet voting, etc.)

- Eligibility of ballot cards scanned for tabulation (i.e., are any eligible ballots excluded, or ineligible ballots included?)
- The selection procedure for the contests chosen to drive the audit
- The status of contests not chosen to drive the audit, especially those with unusual discrepancies, or for which a suitable risk level was not achieved

The protocol below does not address the issues above, but only the correct performance of the Risk Limiting Audit, working from the ballot cards in custody of the Counties, the ballot manifest, and the cast vote record (CVR) files exported from the voting system. A full end-to-end verification of the election would include protocols to check the issues above, in addition to the steps below.

## Protocol Checklist

There are three kinds of items on the checklist below. Observation typically requires a person physically present to see and listen to activities by election officials and other participants. Data requires release of data by election officials. Calculations are performed on data either from election officials or collected by observers, and range from simple line-by-line comparisons to the use of mathematical formulas.

1. **Chain of Custody:** The paper ballot cards selected for audit and reviewed by the Audit Board have not been compromised.
    a. Observation: details of observation depend on local chain of custody protocol. Note that ballots may be remade because of physical damage or other reasons, and the Audit Board should be reviewing the card marked by the voter, which might not be the ballot card scanned.

2. **Tabulation:** Tabulating contests on the CVRs used for the audit yield the announced tabulated results. Requires:
    a. Data: CVR files
    b. Data: Tabulated results for contests selected for audit, from official election results made public by the election agency
    c. Data: Tabulated results exported from RLA tool.
    d. Calculation: tabulate results in contests selected for audit from CVR entries, compare to announced results. These should match. They should also match the tabulated results exported from the RLA tool.
3. **Manifest:** The set of ballot cards listed in each ballot manifest exactly matches the set of ballot cards represented in the corresponding CVR file and exactly matches the physical set of ballot cards. Requires:
    a. Data: The ballot manifest files
    b. Data: The CVR files

   c. Observation: Creation of ballot manifest from the physical set of ballots to be used in tabulation, independent of the vote tabulation system, by observing or reviewing local procedures
   d. Calculation: For each line in the ballot manifest, confirm that all the corresponding CVRs, and no others, are present in the corresponding CVR file.
   e. Calculation: Compare the ballot manifest file uploaded to the RLA Tool to the ballot manifest created from the physical set of ballots, and confirm that these match.
4. **Commitment:** The CVR files and manifest files are finalized before the list of ballot cards is selected for audit. Requires:
   a. Data: Hashes of CVR and ballot manifest files (released to public before selection of random seed and timestamped in a publicly verifiable way)
   b. Data: Ballot manifest files (released to public before selection of random seed)
   c. Data: full CVR files (can be released separately if hashes will match)
   d. Calculation: calculate hashes of the full files and compare to the hashes released before the selection of the random seed. These must match.
5. **Random selection:** Random sequence of ballot cards has been properly selected according to the specified algorithm and seed. Requires:
   a. Observation: Random seed generated at public meeting
   b. Data: Random sequence of ballot cards used for the audit. (Note that this random sequence is generated “with replacement” and thus may include duplicates.)
   c. Data: Ballot manifest file
   d. Data: CVR file
   e. Calculation: Number the ballot card rows of the CVR file sequentially. Then calculate the pseudo-random sequence via the prescribed algorithm based on the random seed. Together these determine the random sequence of ballot cards. This should match the sequence used in the RLA.
6. **Ballot card retrieval:** The list of ballot cards selected for audit matches the set of physical ballot cards actually reviewed by the Audit Board.
   a. Data: CVR file
   b. Data: List of ballot cards assigned for review by Audit Board. This list can be created from the random sequence by removing duplicates.
   c. Observation: physical retrieval and preparation of ballot cards for Audit Board review
7. **Ballot Interpretation and data entry:** Voter intent from ballot is correctly recorded into RLA computer system.
   a. Observation: Observe each audited ballot card and record its marks.
   b. Data: RLA computer system record of voter intent as interpreted by the Audit Board
   c. Calculation: Compare the RLA computer system record of Audit Board interpretations and the direct observation of the audited ballot cards, noting any discrepancies.

8. **Ending the random selection and examination of ballots cards:** : For each contest selected to drive the audit, either the risk limit has been achieved or a hand count has been ordered.

    a. Data: List of contests selected by Secretary of State for audit

    b. Data: status of each contest selected for audit -- in particular, which contests if any have been designated for hand count?

    c. Data: the "risk limit" for each contest selected for audit.

    d. Data: the "error inflation factor" used to calculate whether the risk limit has been achieved. The error inflation factor defines the tradeoff between the sample size with zero discrepancies and the additional sampling needed in the face of discrepancies of different types, and is commonly denoted by the Greek letter gamma (γ).

    e. Data: the "diluted margin" for each contest, i.e., the vote difference between the lowest winning total and the highest losing total, divided by the total number of ballot cards in the county.

    f. Data: for each contest, the number of each type of discrepancy found in that contest by comparing Audit Board interpretations to the original CVR file. These can be calculated by comparing the entries in the CVR file to the corresponding entries in the record of Audit Board interpretations. The types of discrepancies are:

        i. Two-vote overstatements (Audit Board finds a vote for a loser where original CVR showed a vote for a winner)

        ii. One-vote overstatements

        iii. One-vote understatements

        iv. Two-vote understatements

    Note that if a discrepancy shows up on a ballot card which is chosen multiple times, it counts for multiple discrepancies.

    g. Calculation: We can stop auditing a contest when its risk limit has been met. One way to be sure the risk limit has been met is to use the "stopping sample size" given on Stark's Audit Tools web page, which takes the discrepancies found so far (overstatements and understatements) into account. The formula for this stopping sample size is given below. If the size of the sample checked so far equals or exceeds the stopping sample size then the risk limit has been met. With the following notations:

| | |
|---|---|
| a | risk limit |
| g | error inflation factor |
| m | diluted margin |
| $o_2$ | number of two-vote overstatements |
| $o_1$ | number of one-vote overstatements |
| $u_1$ | number of one-vote understatements |
| $u_2$ | number of two-vote understatements |

    the formula for the stopping sample size is:

$$-2g(\log(a) + o_1\log(1-1/(2g)) + o_2\log(1 - 1/g) + u_1\log(1+1/(2g)) + u_2\log(1+1/g)) / m)$$

9. **Hand Count:** Any required hand counts are correctly performed.
10. **Audit Conclusions Affect Outcomes:** Any contests whose outcomes remain in doubt are referred to the proper authority for resolution.
    a. Data: discrepancies, risk levels and results of any hand counts

## **Technical** Notes on Protocol Checklist

### Note on Contests “Selected for Audit”

Under the protocol in Colorado, specified in Rule 25 promulgated by the Colorado Department of State, risk limits are enforced for (and we say the audit is “*driven”* by) certain selected contests. Rule 25 calls these “contests selected for audit.” The other contests are audited, but only “opportunistically”. While discrepancies may be discovered, and risk levels or sample stopping sample sizes calculated for any contest in the election, Rule 25 allows the audit to end based solely on the risk levels in the “contests selected for audit”.

### Note on Hashes and Commitment

Because the CVR and ballot manifest files play a crucial role in the audit, we require a mechanism to ensure that the files being used to verify the audit are the same ones that were committed to before the random selection. “Cryptographic hashing” is a standard mechanism to ensure the integrity of electronic files. If two copies of, say, a CVR file have the same hash, it is virtually certain that the two copies are identical. Because the RLA Tool developed by Free & Fair uses a publicly available hash function (called SHA-256), observers who have the CVR file can calculate its hash and confirm that the CVR file in hand is the one committed to by the election administrators.

### Note on stopping size calculations

Finding “sharper” formulas which can guarantee that the risk limit has been met with smaller sample sizes is an active area of research.

# Other information of interest to the public

- The audit check should ensure that the agreed-upon procedures were used in the audit to handle exceptional cases, such as missing ballots, extra ballots, signature verification failures, etc… - the minimum requirement is that exceptional instances and how they are are handled are described in sufficient detail in publicly available documentation.
- Random seed published by Colorado Department of State (should match random seed generated at public meeting).
- Public participation in generation of random seed
- Round sizes and timing

- Estimated stopping size at intermediate points of the audit
- Evidence that the chain of custody of the paper trail from the voters to the tabulation was really secure and intact: seal protocols, chain of custody, including ballot accounting, and reconciliation with other evidence of how many votes were cast, etc.
- If ballots have been "re-made" (hand-copied so they can be scanned), then both the audit and any check of the audit should be based on the original paper ballot or in some deliberately limited cases an electronic representation of voter intent as produced by the voter before it has been transferred to paper.
- For audits that require software support (instead of just pen and pencil), it should be possible to review the software source code and to re-run the software on the audit data (i.e. the results obtained from hand examination of randomly selected ballots).