Principle 9
AUDITABLE
The voting system is auditable and enables evidence-based elections.

Requirements for Principle 9Principle 9 AUDITABLE The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.1 – Software independence

9.1.1-A – Software independent

9.1.1-B – Paper-based or cryptographic E2E system

9.1.1-C –Mechanism documentation

9.1.2 – Tamper evidence

9.1.2-A – Tamper evident records

9.1.2-B – Tamper-evident record creation

9.1.3 – Voter verification

9.1.3-A – Records for voter verification

9.1.3-B – Identification of errors

9.1.3-C – Ballot error correction

9.1.3-D – Voter reported errors

9.1.4 – Auditable

9.1.4-A – Auditor verification

9.1.4-B – Auditable with compromised software, firmware, or hardware

9.1.4-C – Documented procedure

9.1.5 – Paper records

9.1.5-A – Paper record production

9.1.5-B – Paper record retention

9.1.5-C – Paper record intelligibility

9.1.5-D – Matching selections

9.1.5-E – Paper record transparency and interoperability

9.1.5-F – Unique identifier

9.1.6 – E2E Cryptography

9.1.6-A – Cryptographic E2E transparency

9.1.6-B – Cryptographic verification

9.1.6-C – Ballot receipt

9.1.5-D – Receipt export

9.1.5-E– Mandatory ballot availability

9.1.5-F – Verification of encoded votes

9.1.5-G – Sufficient information for verification

9.1.6 – Audit support

9.1.6-A – Number of ballots to check

9.1.6-B – No fixed margin of error

9.1.6-C – Random number generation

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2-A – Compliance audit procedures

9.2-B – General post-election audit procedures

9.2-C – Generating CVRs

9.2-D – Reporting intermediate results

9.2-E – Reporting unusual audit events

9.2-F – Reporting format

9.2-G – Ballot count

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-A – Data protection requirements for audit records

9.4 - The voting system supports efficient audits.

9.4-A – Efficient compliance audit

9.4-B – Efficient risk-limiting audit

9.4-C – Unique ballot identifiers

9.4-D – Multipage ballots

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.1 – Software independence

9.1.1-A – Software independent

The voting system must be software independent.

Discussion

Software independence means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. All voting systems need to be software independent in order to conform to the VVSG.

There are essentially two issues behind the concept of software independence:

- it is be possible to audit voting systems to verify that ballots are being recorded correctly, and
- testing software is so difficult that audits of voting system correctness cannot rely on the software itself being correct.

Therefore, voting systems need to be 'software independent' so that the audits do not have to trust that the voting system's software is correct. The voting system will provide proof that the ballots have been recorded correctly, ,that is, voting records will be produced in ways in which their accuracy does not rely on the correctness of the voting system's software.

This is a major change from previous versions of the VVSG, because previous versions permitted voting systems that are software dependent, that is, voting systems whose audits rely on the correctness of the software. One example of a software dependent voting system is the DRE, which is now non-conformant to this version of the VVSG.

There are currently two methods specified in the VVSG for achieving independence:

- through the use of independent voter-verifiable paper records, and
- E2E cryptographic voting systems.

Prior VVSG source: 2007 VVSG 2.7-A

9.1.1-B – Paper-based or cryptographic E2E system

Voting systems must meet the requirements within the Paper-based System Architectures or Cryptographic E2E System Architectures section, or both.

Discussion

Both of these architectures are software independent, but they can both be used within the same voting system. In this case, the system would need to be compliant with both sets of requirements.

Applies to:	Voting System

9.1.1-C –Mechanism documentation

A voting system manufacturer must document the mechanism used to provide software independence.

Discussion

Without knowing the specific mechanism, it is difficult to determine if the system truly is software independent.

Applies to:	Voting System
Related requirements:	[TK: Documentation]

9.1.2 – Tamper evidence

9.1.2-A – Tamper evident records

The voting system must produce tamper-evident records that enable detection of incorrect election outcomes, including:

1. capturing the contents of each vote at the time of each ballot's casting, and
2. recording detected errors in a tamper-evident manner.

Discussion

Tamper-evident records include paper ballots and artifacts from an E2E voting system.

The record also ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered.

Applies to:	Voting Device

9.1.2-B – Tamper-evident record creation

A tamper-evident record of the voter's ballot selections must be captured when each ballot is cast.

Discussion

Precinct-based voting systems are the only way to meet this requirement. Entirely separate voting channels, such as remote vote-by-mail, do not offer this opportunity to the voter.

Applies to:	Precinct-based voting systems

9.1.3 – Voter verification

9.1.3-A – Records for voter verification

Tamper-evident records must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections.

Discussion

Precinct-based voting systems are the only way to meet this requirement. Entirely separate voting channels, such as remote postal voting, do not offer this opportunity to the voter.

Applies to:	Vote Capture Devices
Notes:	Barcodes!

9.1.3-B – Identification of errors

The voting system must offer voters the opportunity to identify ballot errors before it is cast.

Applies to:	Paper-based system architectures Cryptographic E2E system architectures

9.1.3-C – Ballot error correction

The voting system must allow a voter to restart a voting session if a ballot is deemed unacceptable.

Applies to:	Paper-based system architectures

9.1.3-D – Voter reported errors

Voting system documentation must describe a method, either through procedural or technical means, for voters to report detected errors or incorrect results.

Discussion

This can include a voter alerting an election worker or pressing a button on the machine to report detected errors or incorrect results.

Related requirements:	[TK: Documentation]

9.1.4 – Auditable

9.1.4-A – Auditor verification

Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated.

Discussion

The voting systems themselves cannot make records available to the public. The manner and decision to make these records available is made by a state and or local jurisdiction. This requirement only ensures that the records themselves are generated and can be easily accessed without additional software or assistance from the voting system manufacturer. This requirement is meant to enable external auditors to perform their own count of the election results.

Applies to:	Voting Device
Related Requirements:	Principle 1 – High Quality Design

9.1.4-B – Auditable with compromised software, firmware, or hardware

The voting system must enable a meaningful audit in the presence of:

1. compromised or malicious software resident on the system
2. compromised or malicious hardware components
3. faults or errors in software components
4. faults or errors in hardware components

Discussion

The production of tamper evidence records protects against this scenario.

9.1.4-C – Documented procedure

The voting system manufacturer must provide a documented procedure to verify that cast ballots were correctly tabulated.

Discussion

This documentation includes procedures and technical practices that verify the results post-election.

Related requirements:	[TK: Documentation]

9.1.5 – Paper records

9.1.5-A – Paper record production

The voting system must produce an independently verifiable paper record of the voter's ballot selections.

Discussion

Voting systems that use independent voter-verifiable records can satisfy the software independence requirement and achieve conformance to the VVSG.

Applies to: Paper-based system architectures

9.1.5-B – Paper record retention

The voting system must retain a paper record of the voter's ballot selections.

Applies to: Paper-based system architectures

9.1.5-C – Paper record intelligibility

The recorded ballot selection must be presented in a way the voter can understand.

Applies to: Paper-based system architectures

9.1.5-D – Matching selections

All representations of a voter's ballot selections produced by the voting system must agree with the selections made by the voter.

Applies to: Paper-based system architectures

9.1.5-E – Paper record transparency and interoperability

All representations of a voter's ballot selections must use an open and interoperable format.

Applies to: Paper-based system architectures

9.1.5-F – Unique identifier

Each paper ballot that is counted may contain a unique identifier, which can be printed on the ballot or affixed by some other external mechanism.

Discussion

Voting systems are not required to affix a unique identifier to ballots, but all voting systems that are certified with risk-limiting audit (RLA) capabilities need to be able to affix a ballot identifier.

Applies to:	Paper-based system architectures
Related requirements:	9.4-B – Efficient risk limiting audit

9.1.6 – E2E Cryptography

9.1.6-A – Cryptographic E2E transparency

The cryptographic E2E protocol used in the voting system must be publicly available, without an explicit request, for open review for 2 years before it enters the voting system certification process.

Applies to:	Cryptographic E2E system architectures

9.1.6-B – Cryptographic verification

Individual voters must have the opportunity to confirm that the voting system correctly interpreted their ballot selections.

Applies to:	Cryptographic E2E system architectures

9.1.6-C – Ballot receipt

After casting, the voter must receive a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system. These receipts

1. do not display any ballot selections made by the voter
2. do not enable the voter to prove their selections on the cast ballot to others
3. are represented in an open and interoperable format
4. contain a unique identifier

Applies to:	Cryptographic E2E system architectures
Related Requirements:	Principle 10 - Ballot Secrecy
	Principle 4 - Interoperable

9.1.5-D – Receipt export

The voting system must be capable of exporting receipt batches in an open format.

Discussion

Voting systems are not required to affix a unique identifier to ballots, but all voting systems that are certified with risk-limiting audit (RLA) capabilities need to be able to affix a ballot identifier.

Applies to: Cryptographic E2E system architectures

Related Requirements: Principle 10 - Transparency

9.1.5-E– Mandatory ballot availability

The voting system must make available all encoded ballots for public posting.

Applies to: Cryptographic E2E system architectures

9.1.5-F – Verification of encoded votes

Voters must have the opportunity to verify that their ballots are included within the tabulation results.

Applies to: Cryptographic E2E system architectures

9.1.5-G – Sufficient information for verification

The receipt must provide sufficient information for voters to verify that their cast ballots are uniquely contained within the publicly available list of encoded ballots.

Applies to: Cryptographic E2E system architectures

9.1.6 – Audit support

9.1.6-A – Number of ballots to check

A voting system manufacturer must document the procedure to determine the number of ballots which need to be checked to reach an election-official-specified margin of error for a given contest.

Discussion

To ensure that the election outcome is correct within a specified margin of error, a minimum number of ballots will be checked. This can be paper records in paper-based system architectures which are checked by election officials, or checks by voters in cryptographic E2E system architectures. This is important to understanding how efficient the system is at detecting changes due to an error or fault.

Related requirements: [TK: documentation requirements]

9.1.6-B – No fixed margin of error

The voting system must allow election officials to determine the margin of error used to determine the number of ballots to check.

Discussion

This requires the documentation of the margins to be specified as an equation rather than having specific margins built into the system. Additional inputs such as margin of victory, total number of voters, number of voters for each candidate, actual ballots, or an audit trail, may be needed to determine the number of ballots needed.

9.1.6-C – Random number generation

If a voting system generates random or pseudo-random numbers, the manufacturer must document the method used to obtain the numbers and how the random numbers are used within the voting system.

Discussion

Various systems used to implement software independence require random numbers, whether for ballot selection for audits or cryptographic purposes.

The most important reason for this requirement is to ensure that cryptographic protocols requiring random numbers use a true random number generator (TRNG) or a cryptographically secure pseudo-random number generator (CSPRNG) as required. For additional information, see NIST SP 800-90A Rev 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators.

Related requirements:	[TK: documentation requirements]
External reference	NIST SP 800-90A Rev 1

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2-A – Compliance audit procedures

The voting system documentation must specify the election procedures necessary to perform a compliance audit.

Discussion

A compliance audit ensures that the election audit trail is sufficiently accurate to reconstruct the outcome according to how voters cast their ballots. Compliance audits provide assurance that a full hand count of the election audit trail shows the outcome according to how the voters really voted.

External references:	Evidence-Based Elections by P.B. Stark and D.A. Wagner
Related requirements:	[TK: documentation requirements]

9.2-B – General post-election audit procedures

The voting system documentation must specify the election procedures necessary to perform a post-election audit.

Related requirements:	[TK: documentation requirements]

9.2-C – Generating CVRs

The voting system must be capable of recording and reporting a cast vote record for each ballot.

9.2-D – Reporting intermediate results

The voting system must be able to report intermediate results as the audit is being conducted.

9.2-E – Reporting unusual audit events

The voting system must be capable of reporting problems as they arise (for example, matching failures).

9.2-F – Reporting format

The voting system manufacturer must document the intermediate and final election audit results in an open format.

9.2-G – Ballot count

Voting systems must count and report the number of ballots cast.

Discussion

This needs to be granular enough to have voting devices and tabulators count and report the number of ballots cast.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-A – Data protection requirements for audit records

All voting systems must meet the requirements listed under Principles 13.1 and 13.2

Related requirements	13.1 and 13.2

9.4 - The voting system supports efficient audits.

9.4-A – Efficient compliance audit

The voting system must produce records to enable an efficient compliance audit.

Discussion

Voting systems need to provide information that will assist election officials in conducting compliance audits, whenever possible. While compliance audits check that procedures are followed, voting systems can provide information that aids in conducting this audit. For example, inspection of event logs is much more efficient if the logs are available in human readable text format. Using event codes in logs, which requires manual decoding, is an example of a record which impairs the efficiency of compliance audits.

9.4-B – Efficient risk-limiting audit

A voting system must produce paper records that allow election officials to conduct an efficient risk-limiting audit.

Discussion

Voting systems contain information which enables election officials to conduct efficient risk limiting audits. For example, by providing a human readable ballot manifest, the voting system makes the process of ballot sampling more efficient.

Applies to:	Optical scanners, BMDs

9.4-C – Unique ballot identifiers

The voting system must enable election auditors to uniquely address individual ballots.

Discussion

This capability is needed to support RLAs.

Applies to:	Auditing system

9.4-D – Multipage ballots

The voting system must be able to appropriately manage multipage ballots during an audit.

Applies to:	Auditing system