Principle 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-A – Software independence

The voting system is software independent.

Applies to: Voting Device

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, one being that it must be possible to audit voting systems to verify that ballots are being recorded correctly, and the second being that testing software is so difficult that audits of voting system correctness cannot rely on the software itself being correct. Therefore, voting systems must be 'software independent' so that the audits do not have to trust that the voting system's software is correct; the voting system must provide proof that the ballots have been recorded correctly, e.g., voting records must 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 must 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: 1) through the use of independent voter-verifiable paper records and E2E cryptographic voting systems.

Status:	New
Updated:	Nov. 3, 2017
Source:	2007 VVSG 2.7-A
Gap notes:	

9.1-B – Tamper evident records

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

Applies to: Voting Device

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

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-B.1 – Voter verification

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

Applies to: Precinct Count Optical Scan and Vote Capture Devices using VVPAT

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

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-B.2 – Tamper-evident record creation

A tamper-evident record of the contents of each vote must be captured at the time of each ballot's casting.

Applies to: Precinct-based voting systems

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

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-B.3 – Tamper-evident record of errors

Detected errors must be recorded in a tamper-evident manner.

Applies to: Voting device

Discussion
This ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered.

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-C – Auditor verification

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

Applies to: Voting device

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 consumed 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.

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-C.1 – Auditable with compromised software or firmware

The voting system must enable a meaningful audit in the presence of compromised or malicious software resident on the system.

Applies to: Voting system

Discussion
The production of tamper evidence records protects against this scenario.

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-C.2 – Auditable with compromised hardware

The voting system must enable a meaningful audit in the presence of compromised or malicious hardware components.

Applies to: Voting device

Discussion
The production of tamper evidence records protects against this scenario.

Status:	New
Updated:	Nov. 3, 2017
Source:	
Gap notes:	

9.1-C.3 – Documented verification procedure

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

Applies to: Voting system

Discussion
This documentation includes procedures and technical practices that need to be informed to verify the results post-election.

Status:	New
Updated:	Jan. 29, 2018
Source:	
Gap notes:	

9.1-C.4 – Auditable with software faults or errors

The voting system must enable a meaningful audit in the presence of faults or errors in software components.

Applies to: Voting device

Discussion

Status:	New
Updated:	Apr. 16, 2018
VVSG 1.1:	
Gap notes:	

9.1-C.5 – Auditable with hardware faults or errors

The voting system must enable a meaningful audit in the presence of faults or errors in hardware components.

Applies to: Voting device

Discussion

Status: New
Updated: Apr. 16, 2018
VVSG 1.1:
Gap notes:

9.1-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.

Applies to: Voting System

Discussion

This may include alerting an election worker, or some input that could be provided to the machine.

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-E – Paper-based or cryptographic E2E system

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

Applies to: Voting device

Discussion

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

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-E.1 – Documentation of mechanism

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

Applies to: Voting device

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

Status: New
Updated: Jan. 29, 2018
Source:
Gap notes:

Paper-based system architectures

The following requirements apply to paper-based voting systems.

9.1-F – Paper record production

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

Applies to: Paper-based system architectures

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

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.1 – Paper record retention

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

Applies to: Paper-based system architectures

Discussion

Status: New
Updated: March 30, 2018
Source:

Gap notes:

9.1-F.2 – Paper record intelligibility

The recorded ballots selection must be presented in a manner understandable by the voter.

Applies to: Paper-based system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.3 – 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

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.4 – Paper record transparency & interoperability

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

Applies to: Paper-based system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.5– Identification of errors

The voter must have the opportunity to identify ballot errors before it is cast.

Applies to: Paper-based system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.6 – 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

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.8 – Unique identifier

Each paper ballot that is counted MAY contain a unique identifier.

Applies to: Paper-based system architectures

Discussion

This requirement is related to 9.4-B. 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 must be able to affix a a ballot identifier.

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-F.8.1 – Unique identifier application

Paper ballot identifiers MAY be printed onto the ballot or affixed via some other external mechanism.

Applies to: Paper-based system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

Cryptographic E2E system architectures

The following requirements apply to voting systems using cryptographic E2E technology.

9.1-G – Cryptographic E2E transparency

The underpinning cryptographic E2E protocol must be publicly available, without an explicit request, for open review for 2 years prior to entering the voting system certification process.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.1 – Cryptographic E2E voter verification

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

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.2 – Opportunity to identify errors

The voter must have the opportunity to identify ballot errors before their ballot is cast.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.3 – Ballot receipt

After inputting ballot selections, the voter receives a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.3.1 – Receipt & ballot secrecy

Receipts provided to voters must not display any ballot selections made by voters.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Notes: Ballot Secrecy

9.1-G.3.2 – Prevention vote buying & voter coercion

Receipts must not enable voters to prove to others their selections on any cast ballots.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017

Source:
Gap notes:

9.1-G.4 – Ballot receipt transparency & interoperability

Receipt data must be represented in an open and interoperable format.

Applies to: Cryptographic E2E System Architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes: Interoperability

9.1-G.4.1 – Ballot receipt identifier

Each ballot receipt must contain a unique identifier.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.5 – Receipt transparency

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

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.6 – Mandatory ballot availability

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

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.7 – 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

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.7.1 – Sufficient information for verification

The receipt provides 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

Discussion

Status: New
Updated: Nov. 3, 2017
Source:
Gap notes:

9.1-G.8 – Additional EAC Requirements

The voting system must meet any other requirements for E2E architectures set forth by the Election Assistance Commission or other certifying body.

Applies to: Cryptographic E2E system architectures

Discussion

Status: New
Updated: Apr 12, 2018
Source:
Gap notes:

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.

Applies to: Voting device

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.

Status: New
Updated: Nov. 29, 2017
Source: N/A
Gap notes:

9.2-B – General post-election audit procedures

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

Applies to: Voting device

Discussion

Status: New
Updated: Nov. 29, 2017
Source: N/A
Gap notes:

9.2-C – Generation of per-ballot CVRs

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

Applies to: Voting device

Discussion

Status: New
Updated: Nov. 29, 2017
Source: N/A
Gap notes:

9.2-D – Reporting intermediate results

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

Applies to: Voting device

Discussion

Status: New
Updated: Nov. 17, 2017
Source: N/A
Gap notes:

9.2-E – Reporting Anomalous Audit Events

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

Applies to: Voting device

Discussion

Status: New
Updated: Nov. 17, 2017
Source: N/A
Gap notes:

9.2-F – Reporting Format

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

Applies to: Voting device

Discussion

Status: New
Updated: Nov. 17, 2017
Source: N/A
Gap notes:

9.2-G – Ballot count

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

Applies to: Voting system

Discussion

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

Status: New
Updated: Jan. 29, 2018
Source: N/A
Gap notes:

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 within 13.1 and 13.2

Applies to: Voting system

Discussion

Status: New
Updated: Apr. 12, 2018
Source:
Gap notes:

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.

Applies to: Voting systems

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. The use of event codes in logs, which requires manual decoding, are an example of a record which impairs the efficiency of compliance audits.

Status:	New
Updated:	Feb. 6, 2018
Source:	
Gap notes:	

9.4-B – Efficient risk limiting audit

A voting device that produces paper records must allow election officials to conduct an efficient risk limiting audit.

Applies to: Optical scanners, BMDs

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.

Status:	New
Updated:	Feb. 6, 2018
Source:	
Gap notes:	

9.4-C – Unique ballot identifiers

Election auditors must be able to uniquely address individual ballots.

Applies to: Auditing system

Discussion

This is a mandatory capability needed to support RLAs.

Status: New
Updated: Nov. 29, 2017
Source:
Gap notes:

9.4-D – Multipage ballots

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

Applies to: Auditing system

Discussion

Status: New
Updated: Nov. 17, 2017
Source:
Gap notes: