Biometric Evidence Standard (BES-1)

NIST / ISO / Regulatory Crosswalk

Issued by	Clavira Standards Program
Document Type	Regulatory / Framework Crosswalk
Version	1.0 · March 2026
Applies	Biometric Evidence Standard (BES-1)
Document ID	BES-RC-1.0

Purpose

This crosswalk maps the Biometric Evidence Standard (BES-1) to selected NIST publications, ISO/IEC standards, and jurisdictional or regulatory source materials relevant to biometric governance.

It is designed to answer a narrow question:

Where does BES-1 address, align with, or remain outside the scope of these frameworks and authorities?

This crosswalk is a reference tool for legal, compliance, privacy, security, and technical stakeholders. It does not determine legal compliance, does not create certification equivalence, and does not imply that any external framework has adopted BES-1.

How to Read This Crosswalk

Each mapped item is assigned one of four postures:

- **BES-1 addresses this:** BES-1 directly defines structural requirements that respond to the expectation.
- **BES-1 addresses this in part:** BES-1 directly addresses a material subset of the expectation, but does not by itself satisfy the full requirement or framework area.
- **BES-1 is compatible with this:** BES-1 aligns with the expectation or can support it, but does not by itself constitute full framework coverage.
- **BES-1 does not address this:** the topic is outside BES-1 scope or requires separate controls, governance, legal analysis, or framework implementation.

This posture model is used throughout the document and is the governing interpretation rule for the crosswalk.

Scope Boundary

BES-1 is an evidence architecture standard. It is not:

- an information security management system,
- an identity-proofing standard,
- a privacy management program,
- a digital-forensics procedure manual,
- a storage-security architecture standard,
- or a legal interpretation by itself.

Accordingly, many mappings in this document are intentionally partial. BES-1 often addresses the evidence and chronology dimension of a requirement while remaining outside broader governance, risk, policy, or technical-control obligations.

Canonical BES-1 Reference Points

The crosswalk uses the following BES-1 anchors:

Core Principles

- Principle 1 — Metadata-Only Evidence
- Principle 2 — Chronological Integrity
- Principle 3 — Purpose Binding at Point of Capture
- Principle 4 — Lifecycle Verifiability
- Principle 5 — Vendor Reconciliation

Integrity Primitives

- Event Attestation
- Anchor to Ledger
- Proof Bundle
- SIEM Reconciliation

Recurring Evidence Artifacts

- Notice artifact
- Consent receipt
- Policy version identifier
- Retention clock context
- Deletion certificate
- Disclosure log
- Vendor confirmation / oversight evidence
- Export log

Part I — NIST Crosswalk

1. NIST SP 800-53 Rev. 5

Crosswalk intent

NIST SP 800-53 Rev. 5 is a broad control catalog for security and privacy controls. BES-1 is not a full control catalog and is not equivalent to NIST control implementation. The mapping below identifies where BES-1 most directly aligns with 800-53 control themes.

NIST 800-53 Theme	BES-1 Posture	BES-1 Anchor	Why
Audit and Accountability (AU)	BES-1 addresses this	Event Attestation; Proof Bundle; SIEM Reconciliation	BES-1 directly structures audit-ready, time-ordered event evidence and exportable records.
Access Control (AC)	BES-1 is compatible with this	Part VI constraints; export integrity; role-based access	BES-1 requires controlled access to evidence and export functions, but does not define a full enterprise access-control regime.
System and Information Integrity (SI)	BES-1 is compatible with this	Chronological Integrity; Anchor to Ledger; SIEM Reconciliation	BES-1 supports tamper-evidence, discrepancy detection, and integrity validation, but does not cover all SI objectives.
Incident Response (IR)	BES-1 is compatible with this	Proof Bundle; SIEM Reconciliation; export logging	BES-1 supports evidence production and investigation, but does not define an incident-response program.
Media Protection / Data Handling (MP)	BES-1 is compatible with this	Metadata-only architecture; export minimization	BES-1 reduces sensitive-data footprint and constrains exports, but does not define full media-security controls.
Planning / Governance (PL, PM)	BES-1 is compatible with this	Governance and Verification	BES-1 provides governance practices for the evidence layer, not a complete management system.
Identification and Authentication (IA)	BES-1 does not address this	Out of scope	BES-1 records evidence about biometric governance; it does not define identity proofing or authenticator requirements.

NIST 800-53 interpretation

BES-1 most strongly aligns with Audit and Accountability and with selected portions of System and Information Integrity. It is not a substitute for a full 800-53 control implementation.

2. NIST SP 800-63-4 Digital Identity Guidelines

Crosswalk intent

NIST SP 800-63-4 addresses digital identity, authentication, enrollment, lifecycle management, and federation. BES-1 does not define digital identity requirements. Its relevance is evidentiary: it helps document how biometric-enabled authentication programs were governed.

NIST 800-63-4 Area	BES-1 Posture	BES-1 Anchor	Complementary Source	Why
Authentication lifecycle management	BES-1 addresses this in part	Event Attestation; lifecycle records	NIST SP 800-63-4	BES-1 can preserve evidence of enrollment, use, and lifecycle governance around authentication events.
Identity proofing / enrollment requirements	BES-1 does not address this	Out of scope	NIST SP 800-63-4	BES-1 does not define how subjects are proofed or enrolled as identities.
Authenticator requirements	BES-1 does not address this	Out of scope	NIST SP 800-63-4	BES-1 does not define biometric authenticator strength or assurance levels.
Federation / assertions	BES-1 does not address this	Out of scope	NIST SP 800-63-4	Federation design is outside BES-1 scope.
Evidence of how authentication was governed	BES-1 addresses this	Event Attestation; Proof Bundle	N/A	BES-1 can document sequencing, consent context, purpose binding, and retention/deletion around biometric authentication events.

NIST 800-63-4 interpretation

BES-1 is complementary to NIST digital identity guidance. It can support auditability and defensibility of a biometric authentication program, but it does not satisfy digital identity guideline requirements by itself.

3. NIST SP 800-92 Guide to Computer Security Log Management

Crosswalk intent

SP 800-92 is highly relevant because BES-1 is built around the proposition that operational logs are necessary but often insufficient for compliance-ready biometric evidence.

NIST 800-92 Theme	BES-1 Posture	BES-1 Anchor	Why
Log generation and retention	BES-1 is compatible with this	SIEM Reconciliation; operational log comparison	BES-1 assumes operational logs exist and can be compared against attested evidence.
Log review / correlation	BES-1 addresses this	SIEM Reconciliation	BES-1 directly structures cross-verification between operational logs and evidence records.
Log integrity	BES-1 addresses this	Chronological Integrity; Anchor to Ledger	BES-1 addresses detectability of retroactive change and integrity assurance of attested events.
Compliance-ready exportability	BES-1 addresses this	Proof Bundle	BES-1 adds exportable evidentiary structure beyond ordinary log management.
Enterprise log-management program	BES-1 does not address this	Out of scope	BES-1 is not a full log-management standard.

NIST 800-92 interpretation

This is one of the strongest mappings in the entire crosswalk. BES-1 can be understood as an evidence architecture layer that sits above ordinary log management and closes gaps that raw logs often leave unresolved.

4. NIST SP 800-207 Zero Trust Architecture

Crosswalk intent

SP 800-207 is not a biometric-governance standard, but it is relevant where biometric systems operate inside modern access environments built around explicit verification, resource protection, and reduced implicit trust.

NIST 800-207 Theme	BES-1 Posture	BES-1 Anchor	Why
Explicit verification / no implicit trust	BES-1 is compatible with this	Event Attestation; purpose and authority binding	BES-1 preserves evidence that governed events were linked to declared authority and purpose.
Resource-focused access posture	BES-1 is compatible with this	Sidecar evidence architecture	BES-1 can operate alongside resource-centric access systems, but does not define zero-trust access design.
Session authorization / policy engines	BES-1 does not address this	Out of scope	BES-1 does not make access decisions or enforce zero-trust policy.
Auditability of access events	BES-1 addresses this	Event Attestation; Proof Bundle; SIEM Reconciliation	BES-1 can document how biometric access-related events were governed and evidenced.

NIST 800-207 interpretation

BES-1 is compatible with zero-trust environments and can strengthen reviewability of biometric-governance events inside them. It is not, however, a zero-trust architecture.

Part II — ISO/IEC Crosswalk

5. ISO/IEC 27001:2022 — Information Security Management Systems

Crosswalk intent

ISO/IEC 27001 defines requirements for an information security management system (ISMS). BES-1 is not an ISMS. Its relevance lies in how it supports evidence, auditability, integrity, and controlled handling of biometric-governance records.

ISO/IEC 27001 Theme	BES-1 Posture	BES-1 Anchor	Complementary Source	Why
Information security governance	BES-1 addresses this in part	Governance and Verification	ISO/IEC 27001:2022	BES-1 defines governance practices for the evidence layer, but not a complete ISMS.
Risk treatment / management system requirements	BES-1 does not address this	Out of scope	ISO/IEC 27001:2022	BES-1 is not a management system standard.
Evidence of control operation	BES-1 addresses this	Proof Bundle; Event Attestation	N/A	BES-1 directly supports production of reviewable evidence showing how biometric governance controls operated.
Access control and auditability around evidence	BES-1 addresses this in part	Part VI constraints; export integrity	ISO/IEC 27002:2022	BES-1 requires controlled access and export logging for the evidence layer.

ISO/IEC 27001 interpretation

BES-1 can support an ISO/IEC 27001 environment by making biometric-governance controls more reviewable, but it is not equivalent to an ISMS and must not be presented as such.

6. ISO/IEC 27002:2022 — Information Security Controls

Crosswalk intent

ISO/IEC 27002 provides control guidance. BES-1 can be mapped to a subset of those control themes, especially logging, access restriction, record integrity, and vendor oversight.

ISO/IEC 27002 Theme	BES-1 Posture	BES-1 Anchor	Why
Logging and monitoring	BES-1 addresses this in part	SIEM Reconciliation; Event Attestation	BES-1 structures logging plus reconciliation for compliance-relevant events.
Access control	BES-1 is compatible with this	Role-based access; export controls	BES-1 constrains access to evidence and export functions, but does not define enterprise-wide access control.
Cryptography / integrity	BES-1 is compatible with this	Anchor to Ledger; cryptographically bound attestation	BES-1 supports integrity assurance and tamper-evidence.
Supplier relationships	BES-1 addresses this in part	Vendor Reconcili-ation	BES-1 directly addresses vendor-side event reconciliation and oversight evidence.
Incident management	BES-1 is compatible with this	Proof Bundle; exportability	BES-1 supports investigation and review but does not define a full incident-management process.

ISO/IEC 27002 interpretation

BES-1 is best understood **as a specialized evidence architecture** that can reinforce selected ISO/IEC 27002 control outcomes in biometric-governance contexts.

7. ISO/IEC 27701:2025 — Privacy Information Management Systems

Crosswalk intent

ISO/IEC 27701:2025 is a privacy information management system (PIMS) standard for PII controllers and processors. BES-1 is not a PIMS, but it strongly aligns with privacy-accountability and evidence themes where biometric data or biometric-governance metadata is involved.

ISO/IEC 27701 Theme	BES-1 Posture	BES-1 Anchor	Complementary Source	Why
Accountability for PII processing	BES-1 is compatible with this	Event Attestation; Proof Bundle	ISO/IEC 27701:2025	BES-1 preserves reviewable records showing what governance actions occurred and when.
Evidence of notice / consent / purpose limitation	BES-1 addresses this in part	Principle 3; notice artifact; consent receipt	ISO/IEC 27701:2025	BES-1 directly structures evidence for these accountability dimensions.
Management system obligations for privacy	BES-1 does not address this	Out of scope	ISO/IEC 27701:2025	BES-1 is not a privacy management system.
Controller / processor evidence and oversight	BES-1 addresses this in part	Principle 5; Vendor Reconcil-iation	ISO/IEC 27701:2025	BES-1 supports controller/processor oversight evidence around biometric workflows.

ISO/IEC 27701 interpretation

This is a strong compatibility mapping, especially for accountability and evidence of privacy-governance execution. BES-1 must not, however, be presented as equivalent to ISO/IEC 27701 certification or full PIMS implementation.

8. ISO/IEC 27037:2012 — Identification, Collection, Acquisition and Preservation of Digital Evidence

Crosswalk intent

ISO/IEC 27037 is highly relevant because it concerns handling of potential digital evidence. BES-1 is not a digital forensics procedure standard, but it is strongly aligned with preservation, chronology, and evidentiary handling logic.

ISO/IEC 27037 Theme	BES-1 Posture	BES-1 Anchor	Complementary Source	Why
Identification of relevant digital evidence	BES-1 addresses this in part	Event Attestation; artifact model	ISO/IEC 27037:2012	BES-1 defines specific evidence artifacts relevant to biometric governance.
Preservation of evidentiary value	BES-1 addresses this in part	Chronological Integrity; Anchor to Ledger	ISO/IEC 27037:2012	BES-1 focuses on preservation of sequencing and integrity.
Collection / acquisition procedures for forensic evidence	BES-1 does not address this	Out of scope	ISO/IEC 27037:2012	BES-1 does not define forensic acquisition procedures or chain-of-custody methods for seized systems.
Documentation of handling and traceability	BES-1 addresses this in part	export logging; attestation; audit-ability	ISO/IEC 27037:2012	BES-1 structures traceability of governance events and evidence exports.

ISO/IEC 27037 interpretation

BES-1 is most **compatible with the preservation and traceability dimension** of digital evidence handling. It does not replace digital-forensics operating procedures.

9. ISO/IEC 27040:2024 — Storage Security

Crosswalk intent

ISO/IEC 27040 concerns storage security. BES-1 is relevant only in the limited sense that it constrains storage of evidence records and reduces biometric-data exposure through metadata-only architecture.

ISO/IEC 27040 Theme	BES-1 Posture	BES-1 Anchor	Complementary Source	Why
Protection of stored information	BES-1 is compatible with this	Metadata-only evidence; controlled exports	ISO/IEC 27040:2024	BES-1 reduces risk exposure in the evidence layer and supports controlled handling of stored evidence records.
Storage architecture security	BES-1 does not address this	Out of scope	ISO/IEC 27040:2024	BES-1 does not define storage-security architecture or implementation controls comprehensively.
Data lifecycle / destruction	BES-1 addresses this in part	Lifecycle Verifiability; deletion certificate	ISO/IEC 27040:2024	BES-1 directly structures evidence of retention and destruction events.
Storage management controls	BES-1 does not address this	Out of scope	ISO/IEC 27040:2024	BES-1 is not a storage-security standard.

ISO/IEC 27040 interpretation

This is a limited compatibility mapping. BES-1 intersects with storage-security concerns where evidence records are stored and exported, but it should not be presented as a storage-security framework.

Part III — Regulatory and Jurisdictional Crosswalk

10. Illinois BIPA

Expectation	BES-1 Posture	BES-1 Anchor	Primary Evidence Artifact
Notice before collection	BES-1 addresses this	Principle 3; Event Attestation	Notice artifact
Written release before collection	BES-1 addresses this	Principle 3; Event Attestation	Consent receipt
Retention schedule upon possession	BES-1 addresses this	Principle 4	Policy version identifier; retention clock context
Destruction on trigger	BES-1 addresses this	Principle 4	Deletion certificate
Disclosure controls	BES-1 addresses this in part	Principle 5; SIEM Reconciliation	Disclosure log
Litigation-ready chronology	BES-1 addresses this	Principle 2; Proof Bundle	Proof Bundle

BIPA Interpretation

BES-1 has one of its strongest direct mappings here because BIPA is sequencing-heavy and litigation-sensitive.

11. Colorado HB 24-1130

Colorado Expectation	BES-1 Posture	BES-1 Anchor	Primary Evidence Artifact
Policy before collection	BES-1 addresses this	Principle 4	Policy version identifier
Notice before consumer collection	BES-1 addresses this	Principle 3	Notice artifact
Opt-in consent before collection or processing	BES-1 addresses this	Principle 3	Consent receipt
Annual review and deletion trigger	BES-1 addresses this	Principle 4	Annual review record; deletion certificate
Processor oversight	BES-1 addresses this in part	Principle 5	Vendor confirmation; disclosure log
AG review / audit-ready chronology	BES-1 addresses this	Principle 2; Proof Bundle	Proof Bundle

Colorado interpretation

BES-1 strongly supports Colorado's time-bound sequencing and review obligations, especially around annual review, deletion triggers, and processor oversight.

12. Federal Financial Services — Theme-Level Supervisory Mapping

This section is thematic rather than authority-by-authority. It synthesizes recurring supervisory and enforcement themes reflected across FFIEC guidance, FTC biometric posture, and broader CFPB consumer-protection relevance. It should not be read as a row-by-row statement of binding federal biometric requirements.

Federal Theme	BES-1 Posture	BES-1 Anchor	Complementary Source	Why
Authentication auditability	BES-1 addresses this in part	Event Attestation; Proof Bundle	FFIEC authentication guidance	BES-1 structures evidence of how biometric authentication was governed.
Monitoring and anomaly detection	BES-1 addresses this in part	SIEM Reconciliation	FFIEC authentication guidance	BES-1 supports discrepancy detection and review.
Vendor oversight	BES-1 addresses this in part	Principle 5	FFIEC third-party risk and supervisory o versight sources	BES-1 supports oversight evidence and reconciliation.
Consumer-protection / fairness inference	BES-1 is compatible with this	Purpose Binding; exportable evidence	CFPB UDAAP posture; FTC Section 5 posture	BES-1 can support defensibility and reviewability where disclosures and governance become contested.
Identity proofing / authenticator assurance	BES-1 does not address this	Out of scope	NIST SP 800-63-4; FFIEC authentication guidance	These are addressed by separate identity and authentication frameworks.

Federal interpretation

BES-1 supports the **evidentiary and auditability dimension** of biometric authentication programs in financial services, but it does not stand in for federal authentication, privacy, or consumer-finance requirements.

Part IV — Optional Future Control Catalog Format

The following format may be used in any future Clavira control catalog or implementation worksheet. It is included here as implementation scaffolding that follows from the crosswalk; it is not itself part of the crosswalk posture model.

Control ID	Control Statement	BES-1 Anchor	Evidence Artifact	Verification Method	Review Cadence	NIST / ISO Family
CLV-EX-01	Notice is evidenced before collection	Principle 3; Event Attestation	Notice artifact	Sample proof-bundle review	Quarterly	800-53 AU / 27701 accountability
CLV-EX-02	Consent is evidenced before enrollment	Principle 3; Event Attestation	Consent receipt	Sequence validation	Quarterly	800-63 lifecycle / 27701 accountability
CLV-EX-03	Deletion is evidenced on trigger	Principle 4	Deletion certifi-cate	Retention-clock audit	Quarterly	800-53 AU/SI / 27037 traceability

This format is illustrative. It should be adapted during control-catalog development, but its structure should remain stable.

Part V — What This Crosswalk Does Not Mean

This crosswalk does not mean:

- BES-1 equals ISO/IEC 27001 certification
- BES-1 equals ISO/IEC 27701 certification
- BES-1 satisfies all NIST identity, logging, or zero-trust requirements
- BES-1 determines legal compliance under BIPA, Colorado law, or federal financial-services regulation
- NIST, ISO, FFIEC, CFPB, FTC, or any state authority has adopted BES-1

Instead, this crosswalk shows where BES-1:

- directly addresses evidence and chronology needs,
- directly addresses a material subset of certain expectations without satisfying the full framework area
- is compatible with broader governance or control frameworks,
- or remains outside their scope.

Conclusion

BES-1 is best understood as a **specialized biometric evidence architecture standard.**

Its strongest mappings are to:

- auditability,
- chronology integrity,
- exportable evidence,
- lifecycle verifiability,
- and vendor-event reconciliation.

Its weakest or out-of-scope areas are:

- management system requirements,
- identity proofing,
- authenticator assurance,
- enterprise storage architecture,
- and full forensic acquisition procedures.

This is an appropriate boundary.

The value of BES-1 is not that it replaces NIST, ISO/IEC, or legal analysis. The value of BES-1 is that it fills a gap those frameworks often leave open in biometric programs: the ability to produce reviewable, time-ordered evidence showing what governance actions occurred, when they occurred, and under what declared authority.