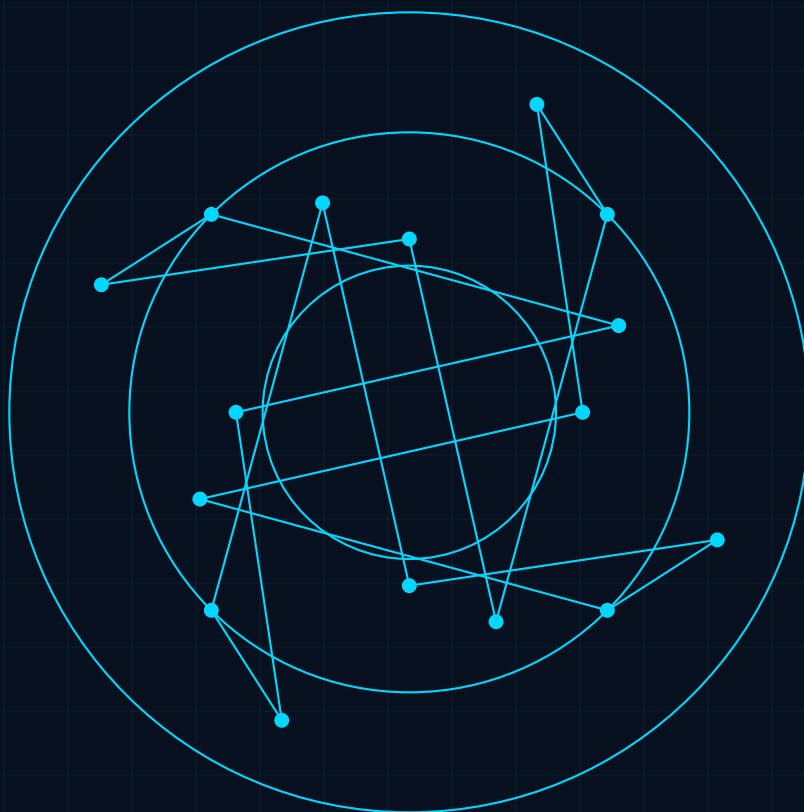


AUTH-001

NIST Current-Version Authority Crosswalk

National Institute of Standards and Technology



MAPPING DOCTRINE

Directional mappings only. No certification, legal compliance, implementation effectiveness, or clause-level equivalence is implied without explicit evidence.

Publication identity

Permanent identity, mapping direction, confidence, and expiration

DOCUMENT ID

AUTH-001

VERSION

2.0.0-candidate

STATUS

Candidate Authority Crosswalk

VALIDATED

2026-09-17

SCHEDULED REVIEW

2026-11-16

AUTHORITY FAMILY

National Institute of Standards and Technology

INTERPRETATION BOUNDARY

This publication is a Mythos-authored crosswalk. External standards remain authoritative only in their official editions. Mappings express relationship and implementation relevance; they are not certifications, legal opinions, or proof that a control is operating effectively.

DIRECTION

External authority -> Mythos publication. Reverse inference is not automatic.

CONFIDENCE

C3 high alignment; C2 strong supporting relation; C1 contextual; C0 no asserted mapping.

EQUIVALENCE

NONE ASSERTED unless a clause-level analysis proves identical scope and obligation.

EXPIRATION

Every mapping expires by date or earlier upon source supersession, material revision, conflict, or implementation change.

Directional mapping method

Five steps prevent crosswalks from becoming false equivalence claims

01 / PIN

Pin exact final version or dated rolling snapshot.

02 / SCOPE

Compare authority purpose, subject, population, system boundary, and obligation type.

03 / MAP

Record only directional relationship to permanent Mythos IDs.

04 / GRADE

Assign C3/C2/C1 confidence and record rationale; equivalence defaults to none.

05 / EXPIRE

Set expiry and event triggers; revalidate before relying on stale mappings.

NON-COMPENSABLE RULE

A high-confidence mapping cannot prove implementation effectiveness. An exact external clause cannot be satisfied merely because a Mythos control has a similar title. Evidence of implementation remains separate from authority mapping.

Current authority/version register

Exact version pins or dated rolling snapshots

ID / SOURCE	VERSION / STATUS	VALID THROUGH
NIST-CSF-2.0 Cybersecurity Framework	2.0 Final	2027-03-16 STABLE
NIST-SP-800-37R2 Risk Management Framework	SP 800-37 Rev. 2 Final	2027-03-16 STABLE
NIST-SP-800-53R5-5.2.0 Security and Privacy Controls	SP 800-53 Rev. 5 / Release 5.2.0 Final update	2026-12-16 MEDIUM
NIST-SP-800-53AR5-5.2.0 Assessing Security and Privacy Controls	SP 800-53A Rev. 5 / Release 5.2.0 Final update	2026-12-16 MEDIUM
NIST-SP-800-171R3 Protecting CUI in Nonfederal Systems	SP 800-171 Rev. 3 Final	2027-03-16 STABLE
NIST-SP-800-171AR3 Assessing CUI Security Requirements	SP 800-171A Rev. 3 Final	2027-03-16 STABLE
NIST-SP-800-172R3 Enhanced CUI Security Requirements	SP 800-172 Rev. 3 Final May 2026	2026-12-16 MEDIUM
NIST-SP-800-172AR3 Assessing Enhanced CUI Requirements	SP 800-172A Rev. 3 Final May 2026	2026-12-16 MEDIUM

Current authority/version register / continued

Exact version pins or dated rolling snapshots

ID / SOURCE	VERSION / STATUS	VALID THROUGH
NIST-SP-800-63-4 Digital Identity Guidelines	SP 800-63-4 Final Jul 2025	2026-12-16 MEDIUM
NIST-SP-800-61R3 Incident Response Recommendations	SP 800-61 Rev. 3 Final Apr 2025	2026-12-16 MEDIUM
NIST-SP-800-218V1.1 Secure Software Development Framework	SP 800-218 v1.1 Final	2027-03-16 STABLE
NIST-SP-800-218A SSDF Community Profile for GenAI / Dual-Use Foundation Models	SP 800-218A Final Jul 2024	2026-12-16 MEDIUM
FIPS-140-3 Security Requirements for Cryptographic Modules	FIPS 140-3 Final	2027-03-16 STABLE
FIPS-201-3 Personal Identity Verification	FIPS 201-3 Final	2027-03-16 STABLE
FIPS-203 ML-KEM Standard	FIPS 203 Final Aug 2024	2027-03-16 STABLE
FIPS-204 ML-DSA Standard	FIPS 204 Final Aug 2024	2027-03-16 STABLE

Current authority/version register / continued

Exact version pins or dated rolling snapshots

ID / SOURCE	VERSION / STATUS	VALID THROUGH
FIPS-205 SLH-DSA Standard	FIPS 205 Final Aug 2024	2027-03-16 STABLE
NIST-AI-RMF-1.0 AI Risk Management Framework + GenAI Profile	AI RMF 1.0 / NIST AI 600-1 Final	2026-12-16 MEDIUM
NIST-PF-1.0 Privacy Framework	1.0 final; 1.1 remains Initial Public Draft Final + draft watch	2026-11-16 HIGH

Directional mapping register

Representative high-value targets; full mapping register accompanies the PDF

NIST-CSF-2.0

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-SEC-0005, MYTHOS-FND-0003, MYTHOS-SEC-0004, MYTHOS-SEC-0007, MYTHOS-SEC-0011, MYTHOS-SEC-0012

Direction: NIST-CSF-2.0 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-37R2

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-FND-0005, MYTHOS-PLT-0005, MYTHOS-SEC-0004, MYTHOS-SEC-0007, MYTHOS-SEC-0011, MYTHOS-CLD-0001

Direction: NIST-SP-800-37R2 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-53R5-5.2.0

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-FND-0003, MYTHOS-CLD-0002, MYTHOS-CLD-0003, MYTHOS-DAT-0003, MYTHOS-ID-0002, MYTHOS-PLT-0002

Direction: NIST-SP-800-53R5-5.2.0 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-53AR5-5.2.0

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-FND-0004, MYTHOS-SEC-0008, MYTHOS-SEC-0015, MYTHOS-SRE-0002, MYTHOS-FND-0001, MYTHOS-FND-0002

Direction: NIST-SP-800-53AR5-5.2.0 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-171R3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-ID-0002, MYTHOS-CLD-0001, MYTHOS-CLD-0002, MYTHOS-CLD-0003, MYTHOS-CLD-0004, MYTHOS-CLD-0005

Direction: NIST-SP-800-171R3 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-171AR3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-FND-0004, MYTHOS-SEC-0008, MYTHOS-FND-0001, MYTHOS-FND-0002, MYTHOS-FND-0003, MYTHOS-FND-0005

Direction: NIST-SP-800-171AR3 -> Mythos. Scope and implementation remain independently assessed.

Directional mapping register / continued

Representative high-value targets; full mapping register accompanies the PDF

NIST-SP-800-172R3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-SEC-0007, MYTHOS-SEC-0017, MYTHOS-CLD-0001, MYTHOS-CLD-0002, MYTHOS-CLD-0003, MYTHOS-CLD-0004

Direction: NIST-SP-800-172R3 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-172AR3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-SEC-0008, MYTHOS-FND-0001, MYTHOS-FND-0002, MYTHOS-FND-0003, MYTHOS-FND-0004, MYTHOS-FND-0005

Direction: NIST-SP-800-172AR3 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-63-4

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-ID-0001, MYTHOS-FND-0001, MYTHOS-FND-0002, MYTHOS-FND-0003, MYTHOS-FND-0004, MYTHOS-FND-0005

Direction: NIST-SP-800-63-4 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-61R3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-SRE-0002, MYTHOS-FND-0001, MYTHOS-FND-0002, MYTHOS-FND-0003, MYTHOS-FND-0004, MYTHOS-FND-0005

Direction: NIST-SP-800-61R3 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-218V1.1

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-PLT-0001, MYTHOS-FND-0005, MYTHOS-PLT-0005, MYTHOS-SEC-0002, MYTHOS-SEC-0014, MYTHOS-SWE-0001

Direction: NIST-SP-800-218V1.1 -> Mythos. Scope and implementation remain independently assessed.

NIST-SP-800-218A

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-AI-0013, MYTHOS-SEC-0002, MYTHOS-AI-0002, MYTHOS-AI-0004, MYTHOS-AI-0009, MYTHOS-AI-0010

Direction: NIST-SP-800-218A -> Mythos. Scope and implementation remain independently assessed.

Directional mapping register / continued

Representative high-value targets; full mapping register accompanies the PDF

FIPS-140-3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-ID-0002, MYTHOS-CLD-0001, MYTHOS-CLD-0002, MYTHOS-CLD-0003, MYTHOS-CLD-0004, MYTHOS-CLD-0005

Direction: FIPS-140-3 -> Mythos. Scope and implementation remain independently assessed.

FIPS-201-3

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-ID-0001, MYTHOS-ID-0002, MYTHOS-SEC-0001, MYTHOS-SEC-0002, MYTHOS-SEC-0003, MYTHOS-SEC-0004

Direction: FIPS-201-3 -> Mythos. Scope and implementation remain independently assessed.

FIPS-203

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-ID-0002, MYTHOS-QTC-0003, MYTHOS-ID-0001, MYTHOS-QTC-0001, MYTHOS-QTC-0002, MYTHOS-SEC-0001

Direction: FIPS-203 -> Mythos. Scope and implementation remain independently assessed.

FIPS-204

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-SEC-0002, MYTHOS-PLT-0001, MYTHOS-PLT-0002, MYTHOS-PLT-0003, MYTHOS-PLT-0004, MYTHOS-PLT-0005

Direction: FIPS-204 -> Mythos. Scope and implementation remain independently assessed.

FIPS-205

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-PLT-0001, MYTHOS-PLT-0002, MYTHOS-PLT-0003, MYTHOS-PLT-0004, MYTHOS-PLT-0005, MYTHOS-PLT-0006

Direction: FIPS-205 -> Mythos. Scope and implementation remain independently assessed.

NIST-AI-RMF-1.0

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-AI-0009, MYTHOS-AI-0001, MYTHOS-AI-0002, MYTHOS-AI-0003, MYTHOS-AI-0006, MYTHOS-AI-0011

Direction: NIST-AI-RMF-1.0 -> Mythos. Scope and implementation remain independently assessed.

Directional mapping register / continued

Representative high-value targets; full mapping register accompanies the PDF

NIST-PF-1.0

C3 / HIGH | EQUIVALENCE: NONE ASSERTED

MYTHOS-FND-0003, MYTHOS-DAT-0003, MYTHOS-FND-0006, MYTHOS-SEC-0005, MYTHOS-SEC-0004, MYTHOS-SEC-0007

Direction: NIST-PF-1.0 -> Mythos. Scope and implementation remain independently assessed.

Confidence and equivalence model

Confidence describes mapping quality, not implementation quality

C3

HIGH ALIGNMENT

Primary-source scope materially overlaps the Mythos obligation or architecture subject. Directional only.

C2

STRONG SUPPORT

Authority informs implementation or assessment but differs in scope, population, granularity, or normative force.

C1

CONTEXTUAL

Useful contextual relationship; should not be used as primary evidence for a requirement.

C0

NO ASSERTED MAP

No mapping is claimed. Absence of a mapping is not evidence of incompatibility.

EXACT-EQUIVALENCE GATE

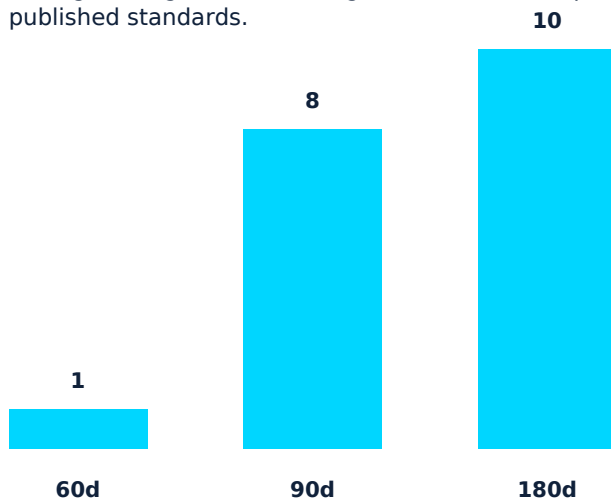
Default state: NONE ASSERTED. Exact equivalence requires clause-level comparison showing the same subject, scope, population, obligation strength, condition, exception set, and assessment expectation. No crosswalk in this release uses exact-equivalence as a shortcut to certification or compliance.

Expiration and revalidation

Every source and mapping has a time horizon and event triggers

SOURCE EXPIRATION DISTRIBUTION

Rolling catalogs, threat intelligence, certification programs, and benchmark result sets expire faster than stable published standards.



SOURCE SUPERSEDED

New revision, errata with normative impact, withdrawn standard, or new final edition.

SCOPE CHANGE

Mythos target changes scope, obligation, assessment method, or permanent identity.

CONFLICT

New authority language contradicts prior mapping assumptions or changes legal/contractual interpretation.

OPERATING CHANGE

Implementation, architecture, population, jurisdiction, or evidence basis materially changes.

Conflicts and explicit limitations

What this crosswalk cannot establish

NO CERTIFICATION

A mapping does not confer external certification, accreditation, authorization, endorsement, or assessor acceptance.

NO LEGAL CONCLUSION

Applicability of statutes, regulations, contracts, procurement clauses, sector rules, and jurisdictions requires separate qualified analysis.

NO EFFECTIVENESS CLAIM

A mapped Mythos control may be designed well and still be absent, misconfigured, stale, bypassed, or ineffective in operation.

NO REVERSE EQUIVALENCE

A Mythos control does not automatically satisfy the external authority merely because the authority maps to it.

VERSION BOUND

The mapping applies to the recorded version or snapshot. Drafts and living registries are explicitly labeled and expire quickly.

CONFLICTS STAY VISIBLE

Where authorities differ, the crosswalk records the disagreement or ambiguity; it does not silently choose the weaker interpretation.

Official source authority register

Primary sources, snapshot date, and validation boundary

NIST-CSF-2.0

Cybersecurity Framework - 2.0

<https://www.nist.gov/cyberframework>

NIST-SP-800-37R2

Risk Management Framework - SP 800-37 Rev. 2

<https://csrc.nist.gov/pubs/sp/800/37/r2/final>

NIST-SP-800-53R5-5.2.0

Security and Privacy Controls - SP 800-53 Rev. 5 / Release 5.2.0

<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

NIST-SP-800-53AR5-5.2.0

Assessing Security and Privacy Controls - SP 800-53A Rev. 5 / Release 5.2.0

<https://csrc.nist.gov/pubs/sp/800/53/a/r5/final>

NIST-SP-800-171R3

Protecting CUI in Nonfederal Systems - SP 800-171 Rev. 3

<https://csrc.nist.gov/pubs/sp/800/171/r3/final>

NIST-SP-800-171AR3

Assessing CUI Security Requirements - SP 800-171A Rev. 3

<https://csrc.nist.gov/pubs/sp/800/171/a/r3/final>

Official source authority register / continued

Primary sources, snapshot date, and validation boundary

NIST-SP-800-172R3

Enhanced CUI Security Requirements - SP 800-172 Rev. 3

<https://csrc.nist.gov/pubs/sp/800/172/r3/final>

NIST-SP-800-172AR3

Assessing Enhanced CUI Requirements - SP 800-172A Rev. 3

<https://csrc.nist.gov/pubs/sp/800/172/a/r3/final>

NIST-SP-800-63-4

Digital Identity Guidelines - SP 800-63-4

<https://csrc.nist.gov/pubs/sp/800/63/4/final>

NIST-SP-800-61R3

Incident Response Recommendations - SP 800-61 Rev. 3

<https://csrc.nist.gov/pubs/sp/800/61/r3/final>

NIST-SP-800-218V1.1

Secure Software Development Framework - SP 800-218 v1.1

<https://csrc.nist.gov/pubs/sp/800/218/final>

NIST-SP-800-218A

SSDF Community Profile for GenAI / Dual-Use Foundation Models - SP 800-218A

<https://csrc.nist.gov/pubs/sp/800/218/a/final>

Official source authority register / continued

Primary sources, snapshot date, and validation boundary

FIPS-140-3

Security Requirements for Cryptographic Modules - FIPS 140-3

<https://csrc.nist.gov/pubs/fips/140-3/final>

FIPS-201-3

Personal Identity Verification - FIPS 201-3

<https://csrc.nist.gov/pubs/fips/201-3/final>

FIPS-203

ML-KEM Standard - FIPS 203

<https://csrc.nist.gov/pubs/fips/203/final>

FIPS-204

ML-DSA Standard - FIPS 204

<https://csrc.nist.gov/pubs/fips/204/final>

FIPS-205

SLH-DSA Standard - FIPS 205

<https://csrc.nist.gov/pubs/fips/205/final>

NIST-AI-RMF-1.0

AI Risk Management Framework + GenAI Profile - AI RMF 1.0 / NIST AI 600-1

<https://www.nist.gov/itl/ai-risk-management-framework>

Official source authority register / continued

Primary sources, snapshot date, and validation boundary

NIST-PF-1.0

Privacy Framework - 1.0 final; 1.1 remains Initial Public Draft

<https://www.nist.gov/privacy-framework>

Use guidance and revision record

A crosswalk is evidence about relationships, not a substitute for assessment

ASSESSMENT USE

1. Confirm the external authority is applicable. 2. Revalidate the exact version or snapshot. 3. Follow the directional mapping to candidate Mythos publications. 4. Examine implementation and operating evidence independently. 5. Record conflicts, exceptions, residual risk, and assessor interpretation. 6. Revalidate before the earliest expiry date.

CURRENT RELEASE

2.0.0-candidate

VALIDATED

2026-09-17

SCHEDULED REVIEW

2026-11-16

PUBLIC IDENTITY

AUTH-001

SOURCE LINEAGE

Regenerated from prior authority-crosswalk source lineage. Permanent public identity remains AUTH-001; the authority register was refreshed on 2026-09-17.