AEA by Ivory & Co.

Trust Architecture Standard

Version: v1.0.0 — Published Anchor: Reliance

1. Definition

Trust Architecture defines the conditions under which reliance between parties is warranted, and how that reliance is established, maintained, changed, transferred, lost and restored over time.

Trust Architecture is the architecture of Reliance.

Its governing question is:

What can be relied upon, under what conditions, and with what authority?

Trust is inherently relational.

It exists because one party may need to rely upon another party, proposition, commitment, action or condition for a particular purpose.

Trust Architecture therefore does not ask whether something is generically “trusted”.

It asks:

Who is relying, upon whom or what, for what, under what conditions, to what extent, and on what basis?

2. Why Trust Architecture Exists

Enterprises operate through reliance.

Customers rely upon businesses.

Businesses rely upon suppliers.

Leaders rely upon people.

People rely upon systems.

Participants rely upon information.

Partners rely upon commitments.

Humans rely upon agents.

Agents may be permitted to act within bounded conditions because relevant parties are prepared to rely upon their operation.

But reliance is never established merely because:

- a Relationship exists;
- a contract exists;
- authority has been granted;
- a control exists;
- a credential exists;
- a system produced an answer;
- a person has performed well before;

· or another party says something should be trusted.

Trust Architecture exists to make the basis and conditions of reliance explicit.

> Trust is not the existence of a relationship. Trust is the warranted reliance that may exist within it.

3. Relational Nature of Trust

Trust requires a relationship of reliance between at least two relevant parties.

At minimum there is:

· a Relying Party; and
· a Relied-Upon Party.

The underlying Actor, Participant, organisation, agent or other party identity remains owned by the relevant source architecture.

Trust owns the reliance proposition between them.

Trust is directional and may be asymmetric.

Party A may rely upon Party B for one purpose while Party B does not rely upon Party A in the same way.

Two parties may also rely upon one another for different attributes, to different extents and under different conditions.

> Mutual Relationship "` symmetrical Trust.

4. Reliance Context

A Reliance Context establishes the bounded proposition within which Trust is being considered.

A useful canonical expression is:

> Party A relies upon Party B for X, under conditions C, to extent E, on basis B.

This structure prevents Trust from being represented as a universal characteristic of a party.

A party may be relied upon:

· for one activity but not another;
· at one transaction value but not another;
· in one Environment but not another;
· with human review but not autonomously;
· for technical accuracy but not commercial judgement;
· or under one set of conditions but not another.

> Trust without context is architecturally incomplete.

5. Reliance Attribute

A Reliance Attribute is the characteristic, quality or behaviour for which reliance is required.

Illustrative attributes may include:

· competence;
· responsibility;
· honesty;
· confidentiality;
· judgement;

- consistency;
- safety;
- delivery;
- discretion;
- accuracy;
- availability;
- loyalty;
- compliance;
- stewardship;
- decision-making;
- autonomous action;
- integrity;
- or another contextually relevant attribute.

This is not a closed taxonomy.

Reliance on one attribute does not imply reliance on another.

> Trust is attribute-specific as well as relational and contextual.

A party may be highly reliable for execution and inappropriate for independent judgement.

Another may be trusted with confidential information but not authorised to commit enterprise funds.

6. Reliance Conditions

Reliance Conditions are the conditions that must hold or remain acceptable for reliance to be warranted.

They may concern:

- identity;
- authority;
- behaviour;
- integrity;
- controls;
- assurance;
- autonomy;
- Environment;
- commitments;
- limits;
- review;
- recovery;
- evidence;
- or another relevant proposition.

The underlying condition remains owned by its source architecture.

Trust owns the reliance consequence of that condition.

> Trust consumes relevant conditions in order to establish Reliance; it does not manufacture another architecture's answer.

7. Conditions of Reliance

Earlier Trust work identified Authority, Control, Assurance, Identity and Autonomy as important

Trust concerns.

These are retained as Conditions of Reliance, not as subordinate AEA architectures.

The established condition families include:

- Identity Conditions
- Authority Conditions
- Control Conditions
- Assurance Conditions
- Autonomy Conditions
- Integrity Conditions

This list is not necessarily exhaustive.

A Reliance Context may require one, several or none of these named condition families depending upon the proposition.

The existence of a condition does not itself establish Reliance.

Trust determines what consequence that condition has for the relevant Reliance Context.

8. Identity Conditions

Identity Conditions concern whether the relevant party, entity, agent, credential or representation is sufficiently established for the Reliance Context.

Trust does not own the underlying Actor or Participant identity.

Ecosystem may own Actor identity.

Workforce may own Participant identity.

Environment may provide identity and access technology.

Intelligence may provide evidence concerning identity.

Reality may capture actual identity-related events or states.

Trust determines whether the identity condition is sufficient for reliance.

> Identity evidence supports reliance. It does not become Trust merely because identity is established.

9. Authority Conditions

Authority Conditions concern whether the relevant party holds the binding decision rights or delegated authority required for the Reliance Context.

Within AEA:

> Workforce Authority Structure owns binding enterprise decision rights.

Authority is held by humans.

Agents may execute delegated authority only within explicitly bounded, machine-enforceable conditions established through Workforce Architecture.

Trust consumes the relevant Authority proposition as a Reliance Condition where authority matters.

> Authority is not Trust.
>
> Being trusted does not confer authority. Being authorised does not establish universal Trust.

An Operational RACI designation does not independently establish binding enterprise Authority.

Technical access does not independently establish Authority.

A Relationship Instrument may establish an obligation or external authority condition without becoming the enterprise's internal Workforce Authority Structure.

10. Control Conditions

Control Conditions concern controls relevant to whether reliance is warranted.

A control may:

- constrain action;
- detect deviation;
- require approval;
- limit exposure;
- preserve evidence;
- enforce separation;
- or otherwise affect the conditions under which reliance can be extended.

Trust does not automatically own the control itself.

The control may be implemented through Execution, Environment, Governance or another owning proposition.

Trust owns the consequence of that control for Reliance.

> A control may support reliance without proving that reliance is warranted in every context.

11. Assurance Conditions

Assurance Conditions concern independent or otherwise established assurance relevant to Reliance.

Assurance may include:

- certification;
- audit;
- accreditation;
- verification;
- professional standing;
- external review;
- testing;
- warranty;
- or another assurance mechanism.

The assurance source may be an Ecosystem Actor.

The evidence and provenance may be established through Intelligence.

Reality may capture actual assurance status.

Trust determines the reliance consequence.

> Assurance can strengthen a Basis of Reliance without becoming the Reliance itself.

12. Autonomy Conditions

Autonomy Conditions concern the bounded independence within which a party or Participant

may act while reliance remains warranted.

Trust may affect whether autonomy is:

- permitted;
- expanded;
- constrained;
- reviewed;
- suspended;
- or withdrawn.

Workforce owns Role, Participant and Authority propositions.

Execution owns the work and instructions.

Environment may enforce technical limits.

Trust owns whether reliance within those bounds remains warranted.

Autonomy is bounded independence. Trust determines whether reliance within those bounds remains warranted.

Autonomy does not itself confer Authority.

13. Integrity Conditions

Integrity Conditions concern consistency between relevant representations and Actuality.

This may include consistency between:

- words and actions;
- promises and delivery;
- Values and behaviour;
- records and practice;
- commitments and decisions;
- representations and Actuality.

The source propositions remain owned elsewhere.

Directional may own Values Guardrails.

Ecosystem may own Relationship Commitments.

Execution may own required work.

Reality captures what actually occurred.

Trust owns the reliance consequence of correspondence or inconsistency.

Integrity is relevant to Reliance because inconsistency can change what a party is warranted in relying upon.

14. Basis of Reliance

The Basis of Reliance records why reliance is warranted or being extended in the relevant context.

It provides relational provenance for Trust.

A Basis of Reliance may include:

- direct experience;
- transferred Trust;

- institutional assurance;
- credentials;
- authority;
- reputation;
- observed behaviour;
- evidence;
- shared Values;
- commitments;
- external information;
- perspective or judgement;
- or another contextually relevant basis.

A Basis of Reliance should remain attributable.

> Trust has relational provenance.

The basis may change over time as direct experience replaces transferred or institutional reliance.

15. Direct Trust

Direct Trust is reliance grounded materially in the relying party's own relationship, experience, evidence or interaction with the relied-upon party.

Direct Trust may strengthen, weaken or become more nuanced as experience accumulates.

Direct does not mean infallible.

A party's interpretation of direct experience may itself be incomplete or mistaken.

Reality captures what occurred.

Intelligence may establish Understanding.

Trust determines the reliance consequence.

16. Transferred Trust

Transferred Trust occurs where reliance is extended partly because an already relied-upon party provides a basis for reliance upon another party.

A canonical pattern is:

> A relies upon B !’ B vouches for C !’ A extends initial reliance to C

Transferred Trust can establish reliance before direct relational history exists.

It remains contextual.

It may be:

- strengthened by subsequent direct experience;
- reduced;
- withdrawn;
- or replaced by another Basis of Reliance.

> Transferred reliance is not universal inheritance of Trust.

The fact that B is trusted for one proposition does not mean every recommendation by B should be relied upon.

17. Transferred Trust and Ecosystem Networks

Transferred Trust may propagate through Ecosystem relationships.

Ecosystem provides the network topology through which that propagation may occur.

Trust owns:

- the Basis of Reliance;
- the transferred reliance;
- the relevant Trust representation;
- Trust Impact;
- and Trust Blast Radius.

Ecosystem shows the network through which reliance may propagate. Trust determines the reliance.

A network connection does not establish Trust.

A referral, introduction, certification or endorsement may provide a Basis of Reliance without proving that reliance remains warranted indefinitely.

18. Trust Indicator

A Trust Indicator is information, observation, experience, perception, event or condition relevant to warranted Reliance.

Trust Indicators may be:

- quantitative;
- qualitative;
- behavioural;
- external;
- perspectival;
- experiential;
- or another relevant form.

Trust owns the meaning of the indicator within the Reliance Context.

Reality may capture the actual underlying event, observation or value.

Intelligence may establish the evidence, provenance, context or Understanding required to interpret it.

Actual event = Reality. Trust relevance = Trust. Reliance consequence = Trust.

A Trust Indicator is not automatically proof.

It contributes to the Basis upon which reliance is assessed.

19. Judgement and Perspectival Indicators

Human judgement may legitimately contribute to Trust.

A person's instinct, concern, confidence or sense that something is wrong may be captured as Perspectival Actuality.

Trust may treat that perspective as a Trust Indicator.

It must not be disguised as objective proof.

Trust Architecture must permit judgement without disguising judgement as mathematical

precision.

The existence of subjective judgement does not invalidate the Trust proposition.

Its basis simply needs to remain visible.

20. Trust Scores

A Trust Score is a governed representation of the condition of Reliance at a defined level and within a defined context.

A Trust Score may be:

- numerical;
- categorical;
- ordinal;
- descriptive;
- or represented through another governed scale.

This Standard does not establish a universal scoring formula.

The score must preserve its Reliance Context, relevant Basis of Reliance and provenance sufficiently to avoid false precision.

> A Trust Score represents Reliance. It is not a generic reputation number.

21. Trust Score Resolutions

The established Trust Score resolutions are:

1. Attribute Trust Score 2. Transaction Trust Score 3. Relationship Trust Score 4. Transferred Trust Score

An Attribute Trust Score represents reliance concerning a particular Reliance Attribute.

A Transaction Trust Score represents reliance in the context of a specific transaction or bounded interaction.

A Relationship Trust Score represents the condition of reliance across a defined Relationship context.

A Transferred Trust Score represents reliance extended through transferred Trust.

A higher-level score is not automatically an arithmetic average of lower-level scores.

> Trust representation is purpose-sensitive.

22. Trust Score and Intelligence Confidence

A Trust Score and an Intelligence confidence representation are different propositions.

Intelligence confidence concerns confidence in the information, evidence, interpretation or Understanding.

Trust Score concerns warranted Reliance between parties in a defined context.

High-confidence information may support a conclusion that Reliance should be low.

Low-confidence information may mean Reliance cannot yet be established.

> Trust Score "` Intelligence confidence score.

Reality may capture the actual value of either representation at a point in time without acquiring

ownership of its meaning.

23. Transactional Trust

Trust may be assessed through individual transactions or bounded interactions.

A useful pattern is:

> Existing Reliance !’ Transaction Conditions !’ Interaction !’ Actuality !’ Trust Impact !’ Subsequent Reliance

The transaction does not automatically reset the whole Relationship.

Its consequence depends upon:

- the Reliance Attribute affected;
- the materiality of the event;
- the existing Basis of Reliance;
- the conditions breached or satisfied;
- and the broader Relationship context.

Transactional Trust allows the architecture to capture local Trust consequences without forcing every interaction into a universal Relationship judgement.

24. Trust Dynamics

Trust changes over time.

Relevant Trust dynamics include:

- Establishment;
- Maintenance;
- Strengthening;
- Degradation;
- Breach;
- Loss;
- Transfer;
- Restoration.

These are not required to operate as a compulsory linear lifecycle.

A Relationship may move between these conditions in different ways.

Different Reliance Attributes may also change independently.

> Trust is dynamic without being forced into a single lifecycle sequence.

25. Trust Breach

A Trust Breach is an event or condition that violates a Reliance Condition.

A breach may concern:

- integrity;
- authority;
- confidentiality;
- performance;
- competence;
- autonomy;

· control;
· assurance;
· commitment;
· or another relevant condition.

Reality captures the actual event or condition.

Trust determines whether it constitutes a breach of the Reliance Context and what impact follows.

A breach does not necessarily destroy all Trust.

26. Trust Loss

Trust Loss is the resulting reduction or withdrawal of Reliance.

Trust Breach and Trust Loss are therefore distinct.

> Breach = violation of a Reliance Condition.
>
> Loss = reduction or withdrawal of Reliance resulting from relevant conditions and judgement.

A severe breach may cause immediate Trust Loss.

A minor breach may cause little or no change.

Repeated small breaches may create substantial degradation.

The Trust consequence depends upon context.

27. Trust Restoration

Trust Restoration is the rebuilding of warranted Reliance after degradation, breach or loss.

Restoration may require:

· changed behaviour;
· evidence;
· remediation;
· assurance;
· control changes;
· reduced autonomy;
· new commitments;
· repeated successful interactions;
· time;
· or another contextually relevant basis.

Restoration is not the erasure of history.

Reality preserves historical Actuality.

Trust determines whether subsequent conditions warrant renewed reliance.

28. Trust Impact

Trust Impact is the change to the conditions or representation of Reliance arising from an interaction, event, new Actuality, new Understanding or changed condition.

Trust Impact may:

· strengthen;

· weaken;
· narrow;
· broaden;
· suspend;
· transfer;
· restore;
· or otherwise alter Reliance.

The underlying event remains owned by its source architecture or Reality as appropriate.

Trust owns its reliance consequence.

29. Trust Blast Radius

Trust Blast Radius is the extent to which a Trust Impact propagates beyond the originating Reliance Attribute, transaction or Relationship.

Established Trust Blast Radius scopes include:

· Local
· Cross-Attribute
· Relationship-Level
· Network

A useful propagation lens is:

> Trust Event !’ Attribute Impact !’ Transaction Impact !’ Relationship Impact !’ Network Impact

This is not a mandatory propagation path.

An event may remain local.

Another may immediately affect the whole Relationship.

Another may propagate through a network through transferred Trust or dependency.

> Trust Blast Radius concerns propagation of Reliance consequence.

This is distinct from any use of “blast radius” in Possibility Architecture, where the concern is the scale of consequence arising from a possible future proposition.

30. Trust Through Time

Trust is temporal because the Basis of Reliance and relevant conditions can change.

Reality owns the actual history through which Trust change can be understood.

Reality may capture:

· events;
· interactions;
· performance;
· breaches;
· restorations;
· perceptions;
· prior Trust Score values;
· and other Trust-relevant Actuality.

Trust determines the reliance consequence of that history.

> Trust changes through time; Reality preserves the Actuality through which that change can

be understood.

Trust history must not be reconstructed by overwriting prior Actuality with the current Trust judgement.

31. Trust and Reality Architecture

Reality captures what is and what was.

Trust determines what can consequently be relied upon.

The governing relationship is:

> Reality captures Actuality !’ Trust determines the Reliance consequence.

Reality does not determine whether Actuality is acceptable or trustworthy.

Trust does not alter Actuality because a party wishes to preserve Reliance.

Trust Indicators and Trust Scores remain Trust-owned propositions.

Reality may capture:

- the underlying event;
- the actual indicator value;
- the actual Trust Score value at a point in time;
- or another Trust-relevant state.

> Trust owns the meaning. Reality captures the Actuality.

32. Trust and Intelligence Architecture

Intelligence establishes the Understanding upon which Trust may depend.

It may provide:

- evidence;
- provenance;
- Source Authority;
- semantics;
- context;
- contradiction;
- confidence;
- derivation;
- Organisational Memory;
- and other relevant Understanding.

Trust consumes that Understanding in order to assess Reliance.

> Intelligence confidence concerns confidence in Understanding. Trust concerns warranted Reliance.

Trust may originate Requirements of Understanding where it needs to understand a Reliance proposition.

Intelligence architects fulfilment of those requirements.

Intelligence does not determine Trust merely because it can establish high-confidence information.

33. Trust and Ecosystem Architecture

Ecosystem owns Actors, Relationships, Exchanges, Dependencies, Relationship Instruments and Relationship Commitments.

Trust owns Reliance.

> The existence of a Relationship does not establish Trust.
>
> The existence of a Dependency does not establish warranted Reliance.
>
> The existence of a contract does not prove performance.

A Relationship Commitment belongs to Ecosystem.

Reality captures actual performance against it.

Trust determines the Reliance consequence.

The governing chain is:

> Ecosystem establishes the Relationship and its commitments !' Reality captures what actually occurs against them !' Trust determines warranted Reliance.

Ecosystem network topology may also establish the pathways through which transferred Trust can propagate.

Trust determines whether and how Reliance propagates.

34. Trust and Workforce Architecture

Workforce owns Role, Participant, Sourcing and the four orthogonal Workforce Structures:

1. Delivery Structure 2. Organisation Structure 3. Authority Structure 4. Discipline Structure

Trust does not own those structures.

The Workforce Authority Structure owns binding enterprise decision rights.

The Workforce Discipline Structure governs competent practice.

Trust may consume propositions from either as Reliance Conditions.

For example:

- professional standing may contribute to a Basis of Reliance;
- authority may be required for a transaction;
- participant competence may affect reliance;
- a delegation boundary may constrain autonomy.

> Competent practice belongs to Discipline. Binding decision rights belong to Authority. Warranted Reliance belongs to Trust.

The four Workforce Structures are orthogonal.

Trust must not imply that Authority outranks Discipline, Delivery or Organisation merely because authority is relevant to a Reliance Context.

35. Trust and Authority

Authority deserves explicit separation because it is frequently confused with Trust.

Within AEA:

> Authority is a Workforce proposition.

Trust may require valid Authority as a Reliance Condition.

For example, a customer may rely upon a representative's commitment only if that representative has authority to bind the enterprise.

But:

> Authority is not Trust.
>
> Being trusted does not confer authority.
>
> Being authorised does not establish universal Trust.
>
> Technical access does not confer authority.
>
> Operational RACI does not by itself constitute the Workforce Authority Structure.

Trust therefore consumes Authority without acquiring it.

36. Trust and Execution Architecture

Execution owns Process Modules, Approved Variants, Tasks, Instructions, Operational Policies, Operational RACI and Operational Metrics.

Trust may constrain how work is performed where Reliance Conditions require:

- additional review;
- human intervention;
- reduced autonomy;
- different approval;
- additional evidence;
- transaction limits;
- escalation;
- or another execution response.

Trust owns the Reliance Condition.

Execution owns the resulting executable work.

> Trust determines warranted Reliance. Execution determines the work response where Reliance Conditions affect work.

A Trust difference does not automatically create an Execution Variant.

Execution determines whether executable instructions materially differ while the Process Module's Canonical Invariant Contract remains intact.

37. Trust and Environment Architecture

Environment owns physical and technological enablement.

Trust may consume Environment propositions as Reliance Conditions.

Relevant conditions may concern:

- access controls;
- security;
- resilience;
- isolation;
- availability;
- technical safeguards;
- physical controls;
- or another enablement proposition.

Environment owns the intended enablement condition.

Reality captures whether it actually holds.

Trust determines whether Reliance is warranted.

Environment establishes the enablement condition !’ Reality captures its Actuality !’ Trust determines the Reliance consequence.

A technically secure Environment does not establish universal Trust.

38. Trust and Directional Architecture

Directional owns strategic intent, choices, commitments, Values Guardrails and other Directional propositions.

Trust may be affected by whether enterprise behaviour corresponds with those representations.

Directional owns the commitment.

Reality captures actual behaviour.

Trust determines the reliance consequence.

Directional establishes the commitment !’ Reality captures what actually occurs !’ Trust determines the Reliance consequence.

Trust may also constrain strategic options where a proposed direction depends upon Reliance that cannot currently be warranted.

That does not transfer the strategic choice into Trust.

39. Trust and Domain Architecture

Domain owns Business Models, Value Chains and Capabilities.

Trust may be a Business Value Anchor where warranted Reliance contributes materially to enterprise value.

A Capability may exist whose outcome supports conditions of Trust.

That does not make the Capability itself a Trust object.

Where a Capability is externally sourced:

- Domain retains Capability identity;
- Workforce owns the sourcing proposition;
- Ecosystem owns the provider Relationship;
- Reality captures actual performance;
- Trust determines warranted Reliance upon the provider.

Trust may affect whether a Capability fulfilment arrangement is relied upon without acquiring Capability identity.

40. Trust and Possibility Architecture

Trust may constrain or expand Optionality.

A possible future may depend upon the enterprise being able to establish sufficient Reliance among relevant parties.

Possibility owns the consequence for future option space.

Trust owns the Reliance proposition.

> Trust condition may constrain possibility. It does not become Possibility-owned.

A hypothetical future Trust state remains a Possibility assumption until the relevant conditions are established.

Trust Blast Radius must also remain distinct from the scale of consequence explored in Possibility.

> Trust Blast Radius = propagation of Reliance consequence.
>
> Possibility consequence = potential impact of a future hypothesis.

41. Trust and Expression Architecture

Expression owns Enterprise Identity and how the enterprise expresses itself to relevant audiences and contexts.

Trust may be affected by correspondence between what the enterprise says or shows and what actually occurs.

The governing chain is:

> Expression establishes what the enterprise says and shows !’ Reality captures what actually occurs !’ Trust determines what can consequently be relied upon.

Expression does not own Trust merely because brand or communication affects reputation.

Trust does not own Expression merely because inconsistency affects Reliance.

42. Trust and AEA Governance

Trust Architecture defines warranted Reliance.

AEA Governance controls authority, versioning, change, conformance, release, archive and governance of the AEA Standards system.

Trust does not replace formal Governance authority.

A party may be trusted and still lack authority to approve an architectural change.

A governance decision may be validly authorised even where a particular party has concerns about Trust.

> Reliance and governance authority are distinct propositions.

Where governance controls or assurance mechanisms affect Reliance, Trust may consume them as Reliance Conditions.

43. Trust and AEA in Action

AEA in Action may combine Trust with other architectures to construct:

- Trust assessments;
- relationship views;
- transaction views;
- delegated autonomy models;
- agent operating models;
- supplier assessments;
- assurance views;

· Trust histories;
· network propagation views;
· or other purpose-specific renders.

Trust contributes:

· Reliance Context;
· Reliance Attributes;
· Reliance Conditions;
· Basis of Reliance;
· Trust Indicators;
· Trust Scores;
· Trust Dynamics;
· Trust Impact;
· and Trust Blast Radius.

Reality contributes Actuality.

Intelligence contributes Understanding.

Ecosystem contributes relationship topology.

Workforce contributes Authority, Discipline, Role and Participant propositions.

Execution contributes work.

Environment contributes enablement conditions.

AEA in Action performs the cross-architecture composition.

The proprietary method of assembling such views is not itself Trust Architecture doctrine.

44. Governing Principles

Trust Architecture is the architecture of Reliance.

Trust Architecture defines the conditions under which reliance between parties is warranted, and how that reliance is established, maintained, changed, transferred, lost and restored over time.

Trust is relational, contextual, attributable and temporal.

Trust without context is architecturally incomplete.

Party A relies upon Party B for X, under conditions C, to extent E, on basis B.

Reliance on one attribute does not imply reliance on another.

Trust consumes relevant conditions; it does not manufacture another architecture's answer.

Identity, Authority, Control, Assurance, Autonomy and Integrity are Conditions of Reliance, not subordinate AEA architectures.

Trust has relational provenance.

Transferred Trust may establish reliance before direct relational history exists.

Ecosystem shows the network through which reliance may propagate. Trust determines the reliance.

Actual event = Reality. Trust relevance = Trust. Reliance consequence = Trust.

Trust Architecture must permit judgement without disguising judgement as mathematical precision.

Trust Score represents Reliance. It is not a generic reputation number.

Trust Score "` Intelligence confidence score.

Breach "` Loss.

Trust changes through time; Reality preserves the Actuality through which that change can be understood.

Trust Blast Radius concerns propagation of Reliance consequence.

Trust Blast Radius "` Possibility consequence scale.

Authority is a Workforce proposition.

Being trusted does not confer Authority. Being authorised does not establish universal Trust.

Technical access "` Authority.

Operational RACI "` Workforce Authority Structure.

Competent practice belongs to Workforce Discipline. Binding decision rights belong to Workforce Authority. Warranted Reliance belongs to Trust.

Relationship existence "` Trust.

Dependency "` warranted Reliance.

Contract existence "` proof of performance.

Expression establishes what the enterprise says and shows. Reality captures what actually occurs. Trust determines what can consequently be relied upon.

45. AI Protocol

AI may assist Trust Architecture by:

- identifying Reliance Contexts;
- identifying candidate Reliance Attributes;
- identifying Reliance Conditions;
- tracing conditions to their source architectures;
- identifying candidate Bases of Reliance;
- distinguishing direct and transferred Trust;
- identifying Trust Indicators;
- identifying possible Trust Impact;
- identifying Trust Blast Radius;
- comparing current and historical Trust representations;
- identifying contradictions between representations and Actuality;
- identifying where Authority has been confused with Trust;
- identifying where technical access has been confused with Authority;
- identifying where a Trust Score has been confused with Intelligence confidence;
- and identifying network pathways through which transferred Trust may propagate.

AI must not:

- infer Trust merely because a Relationship exists;
- infer Trust merely because a contract exists;
- infer Trust merely because a credential exists;
- infer Trust merely because Authority exists;
- confer Authority because a party is trusted;
- infer Authority from Operational RACI;
- infer Authority from technical access;
- treat a control or assurance mechanism as proof of universal Trust;
- convert subjective judgement into objective evidence;

· hide uncertainty through false scoring precision;
· average lower-level Trust Scores into a higher-level score without an established method;
· treat Intelligence confidence as a Trust Score;
· assign Trust Indicator ownership to Reality;
· assign Trust Score ownership to Reality;
· treat historical Trust judgement as historical Actuality without preserving the relevant basis;
· treat Ecosystem network connection as transferred Trust;
· or expose proprietary AEA in Action Trust-assessment methods as Published Standard doctrine.

AI may assist the assessment of Reliance. It must not manufacture Trust, Authority or certainty.

46. Conformance

A conformant application of Trust Architecture must preserve, where applicable:

1. Relying Party; 2. Relied-Upon Party; 3. Reliance Context; 4. Reliance Attribute; 5. Reliance Conditions; 6. relevant Conditions of Reliance; 7. Basis of Reliance; 8. distinction between Direct and Transferred Trust; 9. Trust Indicators; 10. judgement or Perspectival Indicators where material; 11. Trust Scores where used; 12. Trust Score resolution; 13. distinction between Trust Score and Intelligence confidence; 14. Transactional Trust where relevant; 15. Trust Dynamics; 16. Trust Breach where relevant; 17. Trust Loss where relevant; 18. Trust Restoration where relevant; 19. Trust Impact; 20. Trust Blast Radius where relevant; 21. temporal Trust history through Reality; 22. source ownership of Authority; 23. source ownership of Workforce Discipline; 24. source ownership of Environment, Execution, Ecosystem and other Reliance Conditions; 25. distinction between Relationship and Trust; 26. distinction between Dependency and warranted Reliance; 27. Requirements of Understanding originating in Trust where applicable; 28. and separation between native Trust propositions and AEA in Action renders.

47. Non-Conformance

An application is non-conformant where it:

· represents Trust as a universal property without Reliance Context;
· treats mutual Relationship as symmetrical Trust;
· assumes reliance on one attribute implies reliance on another;
· treats Identity, Authority, Control, Assurance or Autonomy as subordinate AEA architectures;
· manufactures source-architecture conditions inside Trust;
· treats a Relationship as proof of Trust;
· treats a Dependency as warranted Reliance;
· treats a contract as proof of performance;
· treats a credential as universal Trust;
· treats Authority as Trust;
· confers Authority because a party is trusted;
· treats Operational RACI as Workforce Authority Structure;
· treats technical access as Authority;
· treats Assurance as Reliance itself;
· treats Autonomy as Authority;
· treats a network connection as Transferred Trust;
· treats a Trust Indicator as proof without regard to context;
· disguises judgement as mathematical certainty;

· treats a Trust Score as a generic reputation score;
· treats a Trust Score as an Intelligence confidence score;
· treats a breach as automatic total Trust Loss;
· treats current Trust judgement as a replacement for historical Actuality;
· uses Trust Blast Radius to mean general future consequence rather than Reliance propagation;
· assigns Trust Indicator or Trust Score ownership to Reality;
· or treats a cross-architecture Trust assessment as a native Trust object merely because Trust is prominent within it.

48. Published Gaps

GAPS — None currently identified that prevent publication of this Standard.

Detailed Reliance Context fields, Reliance Attribute taxonomy, Reliance Condition schemas, Basis of Reliance specification, Trust Indicator classifications, Trust Score scales and calculation methods, Trust Impact methods, Trust Blast Radius protocols, restoration methods and native Trust schematic construction protocols belong in the downstream Trust Architecture package or AEA in Action as appropriate.

No universal Trust Score formula is established by this Published Standard.

The absence of a universal formula is deliberate and does not constitute a doctrine gap.

49. Publication Position

Trust Architecture provides AEA with its architecture of Reliance.

It exists because Trust cannot be reduced to reputation, relationship, authority, control, assurance, confidence or historical performance.

Its core proposition is relational:

Party A relies upon Party B for X, under conditions C, to extent E, on basis B.

The architecture establishes:

· the Reliance Context;
· the attributes for which reliance is required;
· the conditions that must hold;
· the basis upon which reliance is extended;
· the indicators relevant to that reliance;
· the representations through which reliance may be expressed;
· and the way reliance changes, transfers, degrades, propagates and can be restored over time.

It preserves the critical distinctions:

Relationship "` Trust

Dependency "` warranted Reliance

Authority "` Trust

technical access "` Authority

Operational RACI "` Workforce Authority Structure

Assurance "` Reliance

Trust Score "` Intelligence confidence score

Trust Indicator "` underlying Reality event

Breach "` Loss

Trust Blast Radius "` Possibility consequence scale

and:

current Trust judgement "` historical Actuality.

The wider interlock is therefore:

Source architecture establishes the relevant proposition !’ Reality captures what actually occurs !’ Intelligence establishes the Understanding required !’ Trust determines the Reliance consequence.

Where transferred Trust is involved:

Ecosystem provides the network topology !’ Trust determines whether Reliance transfers and how far its consequence propagates.

Where Authority is involved:

Workforce Authority Structure establishes binding decision rights !’ Trust determines whether Reliance upon the authorised party is warranted in the relevant context.

Trust therefore remains dynamic and externally influenced without becoming an owner of the enterprise objects upon which reliance depends.

The governing proposition remains:

Trust Architecture defines the conditions under which reliance between parties is warranted, and how that reliance is established, maintained, changed, transferred, lost and restored over time.