The Trust Formula™

Decomposing Trust as a Measurable, Governed Attribute of the Relationship Between any Two Entities

Scott Foote

Last Updated: 29 June 2026

Phenomenati Consulting
www.phenomenati.com

6 Liberty Square, #2736
Boston, MA 02109
(508) 709-7990 (office)

CONFIDENTIALITY NOTICE: The contents of this document, including any attachments, are intended solely for stakeholders of Phenomenati Consulting, may contain confidential and/or privileged information, and are legally protected from disclosure.

Copyright © 2026 Phenomenati – All Rights Reserved.

<this page is intentionally blank>

Copyright © 2026 Phenomenati – All Rights Reserved.

Contents

Copyright © 2026 Phenomenati – All Rights Reserved.

Trust is not a slogan, a feeling, or a marketing asset.

*It is the operating **permission** that one entity grants another when it is willing to **accept vulnerability under uncertainty**.*

In a digital, automated, and increasingly agentic world, trust must be designed, measured, governed, tested, and repaired over time.

1 Executive Thesis

Trust can be described using a "*formula*": a dynamic assessment of whether entity A *should* rely on entity B for a defined purpose, in a defined context, at a defined point in time. The entities may be persons, companies, governments, AI agents, devices, workloads, APIs, platforms, supply-chain partners, smart contracts, or any other actor capable of making, fulfilling, or violating expectations.[1]

The academic foundation is clear: trust is commonly understood as willingness to be vulnerable under conditions of risk and interdependence, while organizational trustworthiness is often explained through ability, benevolence, and integrity. Those factors remain useful, but they are not sufficient for modern digital enterprise. A trust *decision* now also depends on identity proofing, telemetry, security posture, privacy discipline, explainability, auditability, resilience, lawful processing, redress, and elapsed evidence over time.[2]

The executive move is to make trust *operational*. The Trust Formula is both a conceptual model and an enterprise capability. Conceptually, it characterizes the trustworthiness of a relationship. Operationally, it coordinates the promises, controls, evidence, disclosures, recovery practices, and product behaviors that allow stakeholders to decide whether reliance is justified.

Copyright © 2026 Phenomenati – All Rights Reserved.

2 A Proposed "Trust Formula"

Not to be confused with the "*Trust Equation*" introduced in the book "*The Trusted Advisor*" which describes a framework for improving one's trustworthiness.[3] This proposed "***Trust Formula***" herein is intended as a means to *simplify* the *complexity* of Trust between cooperating business entities, specifically to make this aspect of each relationship concrete, operational, and ***governable***; and that involves several more critical factors (enumerated below) than the psychological "*C's of trust*" discussed in the "*Trust Equation*".

2.1 Decomposing Trust into its Components

For any relationship in which entity A relies on entity B, the "Trust Formula" can be expressed as:

```
T(A->B, c, t) = Wc * H - L
```

Where:

- T is ***trust*** from A toward B;
  - c is the ***context*** or purpose;
  - t is ***time***;
- Wc is the context-specific weighting of factors;
- H is the time-and-history function;
- and L is the exposure, loss potential, or dependency penalty associated with misplaced trust.

What should be obvious with "trust", but is often overlooked… the function is ***directional*** ("A trusts B") and ***contextual*** (for THIS activity, at this TIME, but not THAT activity).

For example:

- an organization may trust a supplier
  - for commodity logistics
  - but not for privileged production access;
- a person may trust an AI assistant
  - to summarize public text
  - but not to authorize a wire transfer;
- a workload may trust an API
  - only for a bounded scope, for a bounded time, under a bounded policy.

Recognizing that each factor is itself a function, a more informative "*formula*" would be:

```
T(A->B, c, t) = Wc { I, C, R, G, B, X, V, S, P, A, Q } * H(A,B,t) - L(c,t)
```

2.2 Conceptual Model, NOT a Mathematical Formula

Like its predecessor from the 1990's, the "Risk Formula"[4], this expression should NOT be misconstrued as an actual mathematical formula. It is simply a pedagogical tool intended as a ***concrete*** expression to simplify and operationalize the ***abstract*** concept of "*Trust*"… decomposing its complexity into discrete components, factors, or topics which may be more actionable.

Note also… this is *deliberately* not a universal score. A single trust number would imply false precision and may result in gross misinformation and potentially misdirection. The purpose of the "*formula*" is ***strictly*** to

Copyright © 2026 Phenomenati – All Rights Reserved.

force *disciplined judgment* (which should be obvious, but too often is interrupted by reckless impulse in pursuit of un-rationalized *speed* or *velocity*):

- What does *success* look like?
- What claims are being made?
- What evidence supports them?
- What *assumptions* are held silently?
- What could fail?
- What does *failure* look like?
- What recourse exists?
- What has happened over time?

Copyright © 2026 Phenomenati – All Rights Reserved.

3 Critical Factors in the "Trust Formula"

3.1 Understanding the Wc {…} Component

This is intended to be more than simply alphabet soup. Wc is intended to represent an important set of explicit, documented governance artifacts (not simply implicit gut call) which… depending upon context… should be important aspects considered in the Trust required by the relationship formed between the two parties:

- ***I*** represents the provider's Identity and Provenance of the services it providers;
- ***C*** represents Capability and Competence incorporating everything from attestation to certification, and relevant experience performing the function to be engaged;
- ***R*** represents Reliability and Consistency covering familiar topics like SLAs, change management discipline, incident history, "drift" monitoring, etc.;
- ***G*** representing Integrity and Rule Alignment exposes reputation, past conduct, governance records, policy adherence, conflict management, ethical reviews, etc.;
- ***B*** representing Benevolence and Legitimate Interest Alignment points to incentive design, fiduciary duties, customer advocacy, misuse/abuse prevention, absence of hidden conflicts, etc.;
- ***X*** represents Transparency and Explainability including things such as plain-language disclosures, explainability of decisions and subsequent actions, transparency into non-human inferencing (e.g., model cards), etc.;
- ***V*** represents Verifiability and Auditability covering from the basics of log sharing, through control testing, third-party audits, assurance reports, evidence rooms, traceability, etc.;
- ***S*** represents Security, Safety, and Resilience attributes of the service to be provided such as secure-by-design, privacy-by-design, zero trust architecture, incident response preparedness and effectiveness, continuity plans, resiliency testing, etc.;
- ***P*** represents Privacy and Data Stewardship looking at the privacy discipline of the service provider including regular and appropriate PIA/DPIAs, maintaining Records of Processing Activities (RoPA), data minimization enforcement, explicit purpose limitation and adherence, retention controls, subject access request handling, etc.;
- ***A*** represents Accountability and Recourse attributes of the dependency/relationship requiring explicit ownership of accountability and responsibility (e.g., RACI matrices) for the intended objectives and outcomes, escalation paths, redress, contractual remedies, post-incident reviews, compensation and/or corrective actions, etc.;
- ***Q*** represents Quality and Fit-for-Purpose of the provider's services during and across the engagement where acceptance criteria are explicit, product quality metrics are monitored and tracked, independent quality reviews are regularly performed, etc.

Not all of these factors will be necessary or critical to every relationship, but all should be considered as Trust is built and continuously reviewed.

Copyright © 2026 Phenomenati – All Rights Reserved.

Factor	Executive Question	Evidence or Operating Signals
Context and Stakes (c)	What purpose is trust being granted for, and how much harm follows if it is misplaced?	Use-case classification, data sensitivity, safety impact, legal duties, dependency analysis, transaction value.
Identity and Provenance (I)	Is B the entity it claims to be, and can its origin, authority, and chain of custody be established?	Identity proofing, device/workload attestation, certificates, signatures, model provenance, supplier registration.
Capability and Competence (C)	Can B perform the task to the required level of quality?	Credentials, testing, evaluations, certifications, experience, operational performance, product quality metrics.
Reliability and Consistency (R)	Does B behave predictably across repeated interactions?	Service levels, defect rates, incident history, drift monitoring, change management, fulfilled commitments.
Integrity and Rule Alignment (G)	Will B honor commitments, policies, law, and stated values when incentives are stressed?	Governance records, policy adherence, conflicts management, ethical review, past conduct.
Benevolence or Legitimate-Interest Alignment (B)	Is B likely to act with appropriate regard for A's legitimate interests?	Incentive design, fiduciary duties, customer advocacy, safety constraints, misuse prevention, absence of hidden conflicts.
Transparency and Explainability (X)	Can A understand what B is doing, why it matters, and when limits have been reached?	Plain-language disclosures, explainability, decision notices, model/system cards, product documentation.
Verifiability and Auditability (V)	Can claims about B be independently checked?	Logs, third-party audits, assurance reports, evidence rooms, traceability, tamper-evident records, control testing.
Security, Safety, and Resilience (S)	Can B resist compromise, fail safely, and recover?	Zero Trust controls, secure design, threat modeling, incident response, continuity plans, resilience tests.
Privacy and Data Stewardship (P)	Does B respect data boundaries and process information lawfully, fairly, transparently, and minimally?	DPIAs, records of processing, data minimization, purpose limitation, retention controls, rights handling.
Accountability and Recourse (A)	When trust is breached, who owns the outcome and how is harm repaired?	Named owners, escalation paths, redress, contractual remedies, post-incident reviews, compensation or correction.
Quality / Fit-for-Purpose (Q)	Does entity B produce outcomes that are accurate, useful, safe, complete, timely, and appropriate for the context in which entity A is relying on it?	Acceptance criteria, product quality metrics, defect rates, error rates, false-positive and false-negative rates, customer outcomes, model evaluation results, service quality, complaint trends, rework rates, safety performance, and independent quality reviews.
Time and Recency-Weighted *Memory* (H)	What does the relationship history show, with recent events weighted appropriately?	Longitudinal performance, recency-weighted incidents, remediation quality, repeated fulfilled promises, decay of stale evidence.
Exposure and Dependency (L)	How dangerous is over-trust in this context?	Blast-radius analysis, concentration risk, privilege level, irreversible action analysis, safety/regulatory threshold.

These factors align with several mature bodies of work. NIST SP 800-207 frames Zero Trust around the premise that implicit trust is dangerous and that access should be continuously evaluated. NIST AI RMF 1.0 identifies trustworthy AI characteristics such as validity and reliability, safety, security and resilience, accountability and transparency, explainability, privacy enhancement, and fairness. NIST CSF 2.0 makes governance explicit through the GOVERN function. GDPR Article 5 makes lawful, fair, transparent, purpose-limited, minimized, accurate, confidential, and accountable processing central to data trust. WEF digital

Copyright © 2026 Phenomenati – All Rights Reserved.

trust work adds practical dimensions such as redressability, auditability, interoperability, and safety.[5][6][7][8][9]

3.2 Understanding the H(A,B,t) Component

In operational terms, H(A,B,t) is *not* the age of the relationship. It is a *recency-weighted memory* of *relevant behavior*:

- fulfilled commitments,
- exceptions,
- breaches,
- near misses,
- remediation quality,
- leadership changes,
- model drift,
- unresolved complaints,
- policy violations, and
- changes in the threat or regulatory environment.

For example:

- a ten-year supplier can become untrustworthy after a material security failure;
- a new partner can be provisionally trustworthy for a narrow, low-risk use case if the evidence is strong and the blast radius is constrained.

3.3 Understanding the L(c,t) Component

In the Trust Formula, L(c,t) represents the exposure, loss potential, or dependency penalty associated with misplaced trust in a specific context at a specific point in time.

It is the part of the model that prevents trust from becoming naïve or excessive: even when an entity appears competent, reliable, secure, accountable, and historically trustworthy, the acceptable reliance decision must still account for what could be lost if that trust proves wrong.

In practical terms, L(c,t) asks: *How dangerous is over-trust here, now?*

The answer depends on factors such as blast radius, privilege level, data sensitivity, concentration risk, reversibility of harm, regulatory consequence, safety impact, autonomy granted, time-criticality, and the availability of recourse.

For example:

- A supplier may be sufficiently trusted for commodity logistics but not for privileged production access;
- an AI assistant may be trusted to summarize public information but not to authorize a wire transfer.

Because both context and time change, L(c,t) is *dynamic*: exposure may rise as dependency deepens, as systems become more interconnected, as threat conditions shift, or as evidence becomes stale.

The executive purpose of L(c,t) is to ***force disciplined judgment*** about *consequence*, not merely *confidence*; it reminds leaders that trust should be *bounded*, *monitored*, and *constrained* by compensating controls such as least privilege, segmentation, human approval, audit logging, redundancy, contractual remedies, fail-safe design, and revocation paths.

Copyright © 2026 Phenomenati – All Rights Reserved.

4 Why Time Belongs Inside the Function

4.1 Time is the Harshest Auditor of Trust

Trust cannot be fully established at onboarding, procurement, hiring, account creation, model release, or first access. At those moments, the relationship has claims, controls, and initial evidence; it does not yet have lived history. Time converts promises into observations.

The *time* factor should have *at least* four properties:

- **Accumulation**
  - Trust should grow when relevant promises are repeatedly fulfilled under ordinary and stressed conditions.
- **Decay**
  - Old evidence should lose weight as systems, people, incentives, ownership, threat conditions, and market pressures change.
- **Asymmetry**
  - Trust usually grows slowly and can collapse quickly, especially after dishonesty, concealment, exploitation, or negligent harm.
- **Repair**
  - After failure, trust cannot be restored by apology alone; it requires accountability, remediation, transparency, changed controls, and enough subsequent time to observe different behavior.

Copyright © 2026 Phenomenati – All Rights Reserved.

5 Trust is Not the Opposite of "Zero Trust"

Zero Trust is often misunderstood as a lack of trust. In reality, it is a control philosophy for safely granting and maintaining trust in hostile or uncertain environments (e.g., "*never trust* [blindly], *always verify*"). A Trust Function should absorb this lesson: trust is not assumed from location, title, brand, tenure, badge, domain name, model label, or vendor logo. It is earned, bounded, continuously verified, and revocable.[5]

For non-person entities, trust is often implemented as policy and proof. A workload trusts another workload because identity, posture, authorization, encryption, telemetry, and policy all agree at that moment. An AI agent is trusted only within a delegated scope, for a defined task, with evidence of model behavior, monitoring, override paths, and accountability. An API is trusted for a transaction because authentication, authorization, schema validation, rate limits, logging, and service obligations are intact.

Copyright © 2026 Phenomenati – All Rights Reserved.

6 The Trust Threshold™: What Level of Trust Is *Sufficient* to Act and Rely Upon?

A Trust *Formula* is incomplete unless paired with a **Trust Threshold**.

The Trust Formula proposed herein characterizes the level of trust between entity A and entity B in a given context and at a given time.

The Trust Threshold concept defines the decision point - the ***minimum* level of trust** required before A *should* rely on B for a particular purpose. The threshold is *conceptual*, circumstantial, and only relevant to each specific relationship dependency.

Reliance should occur only when measured Trust equals or exceeds the trust required for the dependency to be productive and mutually beneficial.

That aligns well with Zero Trust thinking. NIST SP 800-207 describes score-based trust algorithms that compute a ***confidence level*** and grant access *only* when the score exceeds a ***configured threshold*** for the resource; contextual trust algorithms may also consider recent history, behavior, time, and geolocation.[5]

Further, the "threshold" is not fixed, but can be very dynamic over time. It varies according to dependency, consequence, reversibility, regulatory obligation, autonomy, uncertainty, available controls, and the *maturity* and *duration* of the relationship. Further discussion of whether (or not) this "threshold" is actually quantifiable or is purely qualitative is left for another paper.

Copyright © 2026 Phenomenati – All Rights Reserved.

7 From Trust Formula to *Enterprise* Trust *Function*

The proposed Trust Formula also implies an ***organizational* function.** Many enterprises already have the pieces: CISO, CTO, CAIO, DPO, Chief Risk Officer, Product, Legal, Compliance, Safety, Customer Success, Procurement, and Communications. The challenge is often fragmentation. Security says one thing, privacy another, product a third, sales a fourth, legal a fifth, incident response a sixth, etc. Each focused and sometimes fixated on just a few of the critical factors enumerated above. However, the stakeholder(s) experiences all of it *wholistically* as either ***trust*** or ***distrust***.

An *Enterprise* Trust *Function* should not become **another bureaucracy.** It should be a ***coordination*** and ***evidence*** function that answers five questions:

1. What trust promises are we making to customers, employees, partners, regulators, AI users, and machines?
2. What controls, behaviors, and design choices make those promises true?
3. What evidence can stakeholders inspect without theatre or over-disclosure?
4. How do we detect, report, repair, and learn when trust is damaged?
5. How does trust change over time as relationships, systems, people, models, laws, and threats change?

Industry Perspectives on Emerging Digital Trust Practice

WEF has described digital trust as requiring leadership commitment across cybersecurity, privacy, transparency, redressability, auditability, fairness, interoperability, and safety.[10]

ISACA has discussed the rise of the Chief Trust Officer as a role shaped by the need to coordinate trust across digital organizations.[11]

And NIST CSF 2.0 places governance, expectations, policy, and monitoring at the center of cybersecurity risk management.[7]

Copyright © 2026 Phenomenati – All Rights Reserved.

8 A Practical Executive Scorecard

A ***board-level*** **Trust Function scorecard** should be compact and evidence-led**.** It should avoid vanity metrics and instead test whether trust claims remain true under pressure.

Dimension	Board Question	Example Evidence
Promise Integrity	What commitments have we made, and where are they documented?	Public commitments, contracts, privacy notices, trust center, AI disclosures, product terms.
Evidence Freshness	How current is the evidence supporting those commitments?	Audit dates, test recency, unresolved findings, updated DPIAs, AI evaluation cadence, model cards.
Control Health	Are the technical and organizational controls operating effectively?	Control exceptions, access violations, vulnerability exposure, privacy incidents, resiliency tests.
Stakeholder Experience	Are stakeholders able to understand, challenge, and rely on us?	Complaint patterns, sales trust objections, regulator feedback, user appeal outcomes, partner reviews.
Incident Truthfulness	When something goes wrong, do we disclose accurately and repair quickly?	Time to acknowledge, time to contain, root-cause quality, remediation completion, recurrence rate.
Time-Weighted *Trust*	Is trust improving, degrading, or merely assumed?	Trend analysis across incidents, exceptions, renewals, churn, repeated failures, and positive reliance events.

Copyright © 2026 Phenomenati – All Rights Reserved.

9 Implications for AI, Agents, Products, and Ecosystems

9.1 AI Makes the Trust Function *Urgent*

As AI systems become embedded in products and workflows, reliance becomes more complex. Humans may not understand the system, the system may change, and decisions may affect people who never consented to be part of the transaction. NIST AI RMF and OECD AI principles both point toward trustworthiness through governance, transparency, accountability, robustness, privacy, safety, and human-centered values.[6][12]

For product leaders, trust must be designed into the user journey. Users should know when they are dealing with an AI system, what authority the system has, what data is being used, what uncertainties exist, how to challenge an outcome, and how a human accountable party can be reached. For cyber leaders, trust must be bounded by identity, authorization, telemetry, and resilience. For privacy leaders, trust depends on respecting purpose, minimization, transparency, confidentiality, and accountability. For risk leaders, trust is a portfolio of exposures. For boards, trust is an enterprise asset that can be lost through small dishonesties as quickly as through large breaches.

Copyright © 2026 Phenomenati – All Rights Reserved.

10 Closing Thoughts

*Trust is **not a destination** or a **state** to be achieved. It is a continuously evolving **balance** (like **shared capital**) in the relationship between two parties.*

*Like any investment, Trust **grows** over time **like compound interest** based on fulfilled expectations, verified evidence, aligned incentives, and accountable recovery over time.*

*It is also **fragile**: one concealed failure can instantly erase years off from that accumulated shared balance.*

*Given the frontier emerging over the cyber horizon, executives must **stop treating trust as an adjective** and start operating it as a governable attribute of every business-critical dependency/relationship.*

11 Acknowledgements

This article/paper was researched, drafted, and fact checked using a range of AI services, workflows, and agents including ChatGPT, Gemini, Claude, etc. Contributions by the author(s) include the premise, context, topics, outline, prompts, sequencing, experience-based inferences and perspectives, original content, human-created graphics, corrections, verification and validation of conclusions and recommendations, and final review and editing.

12 References

[1] Rousseau, Sitkin, Burt and Camerer, "Not So Different After All: A Cross-Discipline View of Trust" (Academy of Management Review, 1998). https://elearning.unite.it/pluginfile.php/356439/mod_resource/content/0/7.%20Camerer%20-%20Trust.pdf

[2] Mayer, Davis and Schoorman, "An Integrative Model of Organizational Trust" (Academy of Management Review, 1995). https://www.jstor.org/stable/258792

[3] https://trustedadvisor.com/build-trust/trust-equation

[4] Foote and Lynn, “The Risk Formula”,1996, https://www.linkedin.com/pulse/origin-risk-formula-scott-foote-ezuae/)

[5] NIST Special Publication 800-207, "Zero Trust Architecture". https://csrc.nist.gov/pubs/sp/800/207/final

[6] NIST AI Risk Management Framework 1.0. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[7] NIST Cybersecurity Framework 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[8] World Economic Forum, "Earning Digital Trust: Decision-Making for Trustworthy Technologies". https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/

Copyright © 2026 Phenomenati – All Rights Reserved.

[9] World Economic Forum, "Measuring Digital Trust: Supporting Decision-Making for Trustworthy Technologies". https://www.weforum.org/publications/measuring-digital-trust-supporting-decision-making-for-trustworthy-technologies/

[10] World Economic Forum, “Earning Digital Trust – Decision Making for Trustworthy Technologies”, https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/)

[11] ISACA, "How the Rise of the Chief Trust Officer Role Can Shape Digital Trust in Organizations", 2022. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-26/how-the-rise-of-the-chief-trust-officer-role-can-shape-digital-trust-in-organizations

[12] OECD AI Principles overview. https://oecd.ai/en/ai-principles

[13] OECD Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

[14] European Commission, data protection and GDPR principles overview. https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

Copyright © 2026 Phenomenati – All Rights Reserved.

#enterpriseinformation #enterpriseintelligence #trust #digitialtrust #trustops #cybertrustops #CyberSecurity #CyberSecurityOperations #SecurityOperations #SOC #privacy #PrivacyOperations #privacyops #artificialintelligence #ResponsibleAI #AIops #grc #grcops #RiskManagement #CISOLeadership #BoardLeadership #ceo #cio #dpo #cto #ciso #caio #generalcounsel #boardofdirectors #boardroom #Phenomenati #BringingOrdertoChaos

Copyright © 2026 Phenomenati – All Rights Reserved.