KRACH INSTITUTE FOR TECH DIPLOMACY
AT PURDUE



Criteria Provenance

Global Trusted Tech Standard (xGTT)

Version 1.0

The laws, standards and practices behind the xGTT criteria

November 13, 2026

© 2026 Krach Institute for Tech Diplomacy at Purdue

About the Krach Institute for Tech Diplomacy at Purdue

The Krach Institute for Tech Diplomacy at Purdue created and leads the new discipline of Tech Diplomacy, a modern form of statecraft for a world where technology shapes power. The Krach Institute aligns governments, companies, and allies to accelerate the innovation and adoption of trusted technologies that strengthen freedom, security, and prosperity, and resist authoritarian control.

TechDiplomacy.org

© 2026 Krach Institute for Tech Diplomacy at Purdue

The Global Trusted Tech Standard (xGTT) is an open standard published by the Krach Institute for Tech Diplomacy at Purdue (the “Krach Institute”). Use of xGTT is subject to the xGTT Terms of Use available from the Krach Institute and your use of xGTT shall constitute your acceptance of those terms of use. The Krach Institute and affiliated entities disclaim all liability from the use of xGTT and users are advised to follow the standards for fact-based evaluations and may be subject to claims by third parties relating to your evaluation. No evaluation, rating, or score made using xGTT is a substitute for independent due diligence. Anyone considering a transaction or investment, or other decision involving an evaluated government, company, or organization should perform its own independent investigation and analysis and should not rely on any xGTT evaluation for that purpose.

Criteria Provenance

Global Trusted Tech Standard (xGTT)

Version 1.0

Contents

About the Krach Institute for Tech Diplomacy at Purdue..... 2
Contents.....3
What This Document Is.....4
Red-Line Disqualifiers.....4
Democratic Government Trust.....8
Legal & Regulatory Compliance..... 8
Transparency & Disclosures..... 10
Technical Security Practices..... 11
Selected Glossary and References..... 14
Closing Notice.....16

© 2026 Krach Institute for Tech Diplomacy at Purdue

What This Document Is

The Criteria Provenance explains where each criterion of the Global Trusted Tech Standard (xGTT) comes from: the laws, government lists, international standards and established practices of 18 technologically advanced democracies that lead in critical and emerging technology innovation, policymaking, or both. They are Australia, Canada, Denmark, Estonia, Finland, France, Germany, India, Israel, Japan, the Netherlands, New Zealand, South Korea, Sweden, Switzerland, Taiwan, the United Kingdom, and the United States, referred to throughout xGTT as the "xGTT democracies." Their laws are not identical, but together they provide a body of real-world practice that xGTT draws on in place of an abstract definition of trust. This document is written for policymakers, procurement officials, companies, researchers and anyone asking why a criterion exists.

This document is an explanatory companion to the xGTT Standard. It records the origins of the criteria; it does not describe how an evaluation is conducted, which is set out in the Methodology Guide, and creates no additional requirement, threshold or verdict. The criteria themselves are defined in the xGTT Standard, which governs wherever this document differs from it.

xGTT Version 1.0 is published as four companion documents: the xGTT Standard, which defines the 31 criteria and what a company is expected to demonstrate for each; the Methodology Guide, which sets out how an evaluator applies the criteria to a company using public evidence; the Criteria Provenance (this document), which shows the laws, standards and practices behind each criterion; and the Frequently Asked Questions (FAQ), which answer common questions about xGTT. Where any of the other documents differs from the xGTT Standard, the xGTT Standard governs.

xGTT evaluations are built around an AI-prepared draft and human review. An evaluator may use an AI model to research the public record and prepare the report, following the Methodology Guide. The result is a draft until a person has reviewed it, checking the evidence and every verdict, and only a reviewed report should be relied on.

Using this companion

References below explain the Standard's rationale and are not substitutes for current source verification. Laws and frameworks cited here must be checked for current applicability before they are relied on as evidence about a company. As the xGTT Standard sets out, an evaluation examines the public record of the company's home country and of the xGTT democracy where it has its largest operations, together with the principal sanctions and export-control lists of the xGTT democracies. That scope is drawn where a company is most exposed to democratic oversight.

How to read each entry

Each entry has the Red Line or criterion's ID and name, followed by up to five parts.

"What it checks" says in plain words what the evaluator looks for. "Why" explains the reason the rule exists. Both are simplified: the full requirement, including thresholds and exceptions, is set out in the xGTT Standard.

"How it is evaluated" points to the criterion with the same ID in the xGTT Standard (for example, RL1 for RL1 — Sanctioned Entity). The rules an evaluator applies to reach a verdict on that criterion are in section 08 (Criteria Rules) of the Methodology Guide. The Standard states what a company is expected to demonstrate, what kind of evidence counts and when a criterion is not applicable. Where a summary here differs from the Standard, the Standard governs.

"Anchors" lists the laws, government lists and established practices in the 18 xGTT democracies that the criterion is based on. They are not a checklist, and meeting a listed law does not by itself satisfy the criterion. Some entries add background on how the rule was drawn.

Red-Line Disqualifiers

Ten Red Lines. Each involves conduct or status so fundamentally incompatible with trust that failing even one ends the evaluation: the company is disqualified and the remaining criteria are not assessed. Disqualification lifts

© 2026 Krach Institute for Tech Diplomacy at Purdue

only when the underlying matter is formally resolved. An UNCLEAR verdict on a Red-Line criterion does not end the evaluation. Allegations and pending matters alone do not cause a Red-Line failure.

RL1. Sanctioned Entity

What it checks: Whether the company is on a government sanctions list that blocks its dealings or freezes its assets, or is treated as blocked because a sanctioned party owns or controls it.

Why: A sanctions designation is a government's formal decision to cut an entity off from its economy. Where a government's own sanctions law extends that decision to companies owned or controlled by a sanctioned party, xGTT follows that government's rule and adds none of its own.

How it is evaluated: see RL1 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US OFAC Specially Designated Nationals (SDN) List; EU Consolidated Financial Sanctions List; UK Sanctions List (OFSI); the US OFAC 50 Percent Rule and the EU and UK sanctions ownership-and-control tests.

RL2. Conduct-Based Export Control Violation

What it checks: Whether the government of an xGTT democracy has restricted the company for its own export-control conduct, for example by listing it on the US Entity List for what it did, or has formally found that the company broke its export-control law.

Why: Export controls keep sensitive technology away from uses that democracies prohibit. A company that a government itself has found to have broken those rules has shown it cannot be trusted with controlled technology.

How it is evaluated: see RL2 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US Export Administration Regulations, 15 CFR Part 764 (violations, civil penalties, denial orders, and criminal sanctions); US BIS Entity List and Denied Persons List, including Entity List entries whose stated basis is the entity's own conduct, human-rights-related conduct included (assessed under RL2, not RL7); UK HMRC compound settlements (offered for inadvertent breaches that the exporter voluntarily disclosed, with an admission, a payment, and publication); EU Dual-Use Regulation 2021/821; UK Strategic Export Control Lists; Australia Defence and Strategic Goods List (DSGL). Each xGTT democracy's own restricted-party lists count under RL2 where the stated basis of the listing is the company's own conduct.

Why these limits: governments themselves separate knowing or willful violations from inadvertent and administrative ones, and settle voluntarily disclosed inadvertent breaches on lighter terms, so xGTT relies on what the government's own published record says rather than on its own view of intent. Governments also differ, and change course, on whether a company owned by a restricted party is itself restricted: the US Entity List "Affiliates Rule," issued September 29, 2025, was suspended for a year from November 10, 2025. Because this treatment differs and changes, xGTT adds no ownership rule of its own to RL2; an ownership-only restriction is reported as context or assessed under RL3.

RL3. Authoritarian State Ownership or Control

What it checks: Whether the company is controlled by a government that at least two xGTT democracies formally identify as an adversary and that is rated Not Free in Freedom House's *Freedom in the World* report. Every evaluation records whether, and by which government, the company is controlled. Where control is established but the check on the controlling government cannot be completed, the verdict is UNCLEAR.

Why: A company controlled by a hostile authoritarian government can be directed to act for that government — to hand over data, build in access or withhold service — whatever its own intentions. Requiring formal identification by democratic governments keeps the test tied to their decisions rather than to xGTT's own judgment.

How it is evaluated: see RL3 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: formal adversary determinations made by the governments of the xGTT democracies (for example, in the U.S., the foreign-adversary determinations under 15 CFR Part 791; in the U.K., the enhanced tier of the

© 2026 Krach Institute for Tech Diplomacy at Purdue

Foreign Influence Registration Scheme); 31 CFR Part 800 (CFIUS's regulatory definition of "control," the source for the Standard's governance-rights test); UK National Security and Investment Act 2021; Australia FIRB National Security Review.

Illustrative applications: a 2024 executive-branch market-access prohibition against a cybersecurity software vendor came with an explicit government finding that the vendor's home government had "the capacity to influence or direct" its operations. A national-security agency determination of that kind satisfies the control test directly, even with no confirmed equity stake; whether it is disqualifying then depends on whether at least two xGTT democracies formally identify that government as an adversary and it is rated Not Free. By contrast, a 2024 legislative designation of a named social-media platform as controlled by a foreign adversary does not, standing alone, establish control: it rests on a lower ownership threshold than the control test and lacks an attributed agency assessment. A 2018 decision by one xGTT democracy, informed by its signals-intelligence agency's guidance, to bar telecom-equipment vendors headquartered in one country from its 5G network is a high-risk-vendor finding of the type that counts as formal identification, and a reminder that such findings may not appear in any single country's sources. Finally, a company majority-owned by an authoritarian government that does not meet this test is not disqualified: the ownership is disclosed and the company is evaluated on its conduct like any other.

RL4. Espionage or IP Theft Conviction

What it checks: Whether the company, or a senior officer acting in a controlling role, has been convicted of economic espionage or criminal trade-secret theft, or has formally admitted it, for example through a guilty plea or deferred prosecution agreement. Ordinary civil intellectual-property disputes are covered by LC4.

Why: Stealing technology secrets, often for a foreign state, directly threatens the partners and governments a trusted supplier serves. A conviction or formal admission is the clearest public proof.

How it is evaluated: see RL4 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US Economic Espionage Act (18 U.S.C. §§ 1831–1832); WTO TRIPS Art. 61; EU Trade Secrets Directive 2016/943; Japan Unfair Competition Prevention Act.

RL5. Critical Infrastructure Sabotage Finding

What it checks: Whether a court or government has found that the company knowingly damaged, disrupted or interfered with critical infrastructure — such as energy, water, telecommunications, transportation or finance — in an xGTT democracy. Being the victim of an attack, or an ordinary outage, does not count.

Why: Suppliers to critical infrastructure are trusted with systems society depends on. A company found to have sabotaged them cannot hold that trust.

How it is evaluated: see RL5 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: CISA official attributions; EU Cyber Diplomacy Toolbox; NATO Cyber Defence Policy.

RL6. Terrorism Financing Designation

What it checks: Whether the government of an xGTT democracy, or the European Union, has formally designated the company, or a company it controls, under its counter-terrorism-financing laws.

Why: A terrorism-financing designation is a government's formal finding that dealing with the entity helps fund terrorism. Nothing else in an evaluation can offset it.

How it is evaluated: see RL6 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US OFAC Specially Designated Global Terrorist (SDGT) List; EU Terrorist List (CFSP 2001/931).

RL7. Systematic Human Rights Abuse

What it checks: Whether a democratic government has taken formal action against the company, such as a sanction, and stated in its official reasons that the company was involved in systematic human-rights abuse. Allegations and NGO reports alone do not count. An Entity List listing for the company's own conduct is assessed under RL2.

© 2026 Krach Institute for Tech Diplomacy at Purdue

Why: Technology can be used to enable mass repression. When a democratic government formally names a company for that role, xGTT treats the government's finding as decisive rather than weighing the evidence itself.

How it is evaluated: see RL7 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: EU Global Human Rights Sanctions Regime; UK Global Human Rights Sanctions Regulations; US Global Magnitsky Sanctions. An Entity List listing based on the entity's own conduct is assessed under RL2, not here.

RL8. Prohibited Military End-Use Transfer

What it checks: Whether a court, a formal admission or a confirmed enforcement action has established that the company knowingly supplied controlled technology for a prohibited military use or to a prohibited military user. Paperwork or license-condition failures alone do not count.

Why: Diverting controlled technology to prohibited militaries is among the gravest harms export controls exist to prevent. RL2 covers export violations generally; RL8 singles out this one.

How it is evaluated: see RL8 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US BIS Military End-User (MEU) List; Wassenaar Arrangement; Missile Technology Control Regime (MTCR); UK Export Control Act 2002.

RL9. Unauthorized AI Model Weight Acquisition or Distribution

What it checks: Whether a court, or the company's own admission, has established that it knowingly built on, distributed or sold AI model weights unlawfully taken from another developer. Distillation from a model's lawfully accessed outputs does not count. This criterion applies to every company, not only frontier AI developers.

Why: Model weights are the core asset of an AI developer. A company that trades in stolen weights undermines the security of the whole AI supply chain.

How it is evaluated: see RL9 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US Defend Trade Secrets Act (18 U.S.C. § 1836); Computer Fraud and Abuse Act (18 U.S.C. § 1030); EU Trade Secrets Directive 2016/943.

A known detection limitation: detecting this conduct depends almost entirely on non-technical evidence — litigation, a formal admission or credible investigative reporting — because no generally reliable technical method can prove that a set of weights derives from a specific unlawful source once it has been fine-tuned. Hash-matching does not survive retraining, and behavioral fingerprinting is circumstantial at best. The absence of a technical forensic finding is therefore not evidence of absence; the rarity of findings under this Red Line likely reflects a detection gap rather than rare misuse.

RL10. Non-Consensual or Child-Sex-Abuse Generating AI

What it checks: Whether a court, regulator or the company's own admission has established that it knowingly built, deployed or sold an AI system whose main or marketed purpose is to generate non-consensual intimate images of real people or child sexual abuse material, where that is prohibited. Misuse of a general-purpose tool against its terms, despite reasonable safeguards, does not count, and unlawful purpose is not inferred from capability alone.

Why: These systems cause severe harm to real people and are prohibited across the xGTT democracies. Knowingly offering one is incompatible with trust.

How it is evaluated: see RL10 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: EU Directive 2024/1385, Art. 5 (Non-Consensual Intimate/Manipulated Material); US TAKE IT DOWN Act (2025); UK Online Safety Act 2023 (Non-Consensual Intimate Image Offenses).

© 2026 Krach Institute for Tech Diplomacy at Purdue

Democratic Government Trust

This dimension recognizes that a democratic government's decision to vet, contract with or invest in a company, with real accountability at stake, is strong and independent evidence of trustworthiness — evidence that exists regardless of what the company publishes about itself. Where no such relationship is plausible for a company, the dimension is treated as not applicable rather than counted against it.

GT1. Democratic Government Contract Trust Standing

What it checks: Whether the government of an xGTT democracy, or NATO, buys from the company or has vetted it — through a public contract, grant or authorization, or a security-vetted arrangement such as a defense or government-cloud accreditation. Not applicable where no such relationship is plausible.

Why: A government that buys from or vets a company has checked it with real accountability at stake. That is independent evidence of trust that does not depend on what the company says about itself.

How it is evaluated: see GT1 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: NATO NCIA approved vendor list; FedRAMP High/Moderate; US DoD CMMC; Japan ATLA; Australia DISP; Canada Contract Security Program (PSPC); UK Cyber Essentials Plus / G-Cloud; Germany BSI classified-government certification; South Korea DAPA; Israel DDR&D/MAFAT.

Examples of qualifying relationships: GT1 is one test — does the public record confirm a government relationship in an xGTT democracy? Relationships range from heavily vetted to ordinary purchases. The range shows depth of vetting but does not change the verdict: any confirmed relationship qualifies. Intelligence, NATO and critical-infrastructure relationships (anchors: NATO NCIA approved vendor list; FedRAMP High). Defense-industrial relationships (anchors: US DoD CMMC; German BSI classified-government certification; Australia DISP; Japan ATLA; FedRAMP Moderate). General government purchases of ordinary technology products or services (anchors: EU procurement notices (TED); UK Cyber Essentials Plus; France SecNumCloud; Israel INCD). A classified relationship is not inferred: if no public record confirms it, the company may supply the record that confirms it.

GT2. Strategic Equity Standing

What it checks: Whether the government of an xGTT democracy holds shares in the company, directly or through a vehicle it takes part in. Passive holdings by public pension funds or central banks do not count. The criterion applies to the same companies as GT1 and is not applicable where GT1 is not.

Why: A government that puts public money into a company has already examined it, and that is the signal this criterion records; the size of the stake or its governance rights does not change the signal. Holdings by governments outside the xGTT democracies are disclosed separately and do not satisfy this criterion.

How it is evaluated: see GT2 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: Japan METI strategic-equity context; US CHIPS and Science Act strategic-equity provisions.

Legal & Regulatory Compliance

Four criteria about whether a government or court has made a final finding against the company — for corruption, fraud, privacy violations or intellectual-property infringement — within five years of resolution. Allegations, open investigations and private lawsuits are reported as context, not counted. A past finding can be cleared where the company's remediation is confirmed: the conduct has ended and the underlying deficiency has been corrected. Payment of a fine, penalty or judgment alone is not remediation.

LC1. No Major Corruption Conviction

What it checks: Whether the company has been convicted of corruption, such as bribery, or has resolved a criminal corruption case through a guilty plea or a deferred or non-prosecution agreement, within the look-back period.

© 2026 Krach Institute for Tech Diplomacy at Purdue

Why: A corruption conviction shows a company has won business by improper means. Democratic governments themselves debar companies for it.

How it is evaluated: see LC1 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: OECD Anti-Bribery Convention Art. 3; World Bank Debarment List; CFIUS; UK Serious Fraud Office (SFO); France Parquet National Financier; South Korea Anti-Corruption and Civil Rights Commission (ACRC); Australia National Anti-Corruption Commission (NACC); EU OLAF.

LC2. No Major Fraud Enforcement Action

What it checks: Whether a government has taken final enforcement action against the company for securities or financial fraud within the look-back period. Open investigations and private lawsuits are reported as context.

Why: Fraud findings go to whether a company's own statements can be relied on. The criterion rests on what a government has finally determined, like the rest of this dimension.

How it is evaluated: see LC2 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: FATF Recommendations; SEC Enforcement Actions; UK FCA Enforcement; Japan FSA; Germany BaFin; Israel Securities Authority (ISA); India SEBI; Australia ASIC.

LC3. No Repeated Privacy Enforcement

What it checks: Whether data-protection regulators have penalized the company repeatedly, or once for a severe violation, within the look-back period.

Why: Any large company may face an occasional privacy fine. A pattern of significant penalties, or one severe penalty, shows that personal data is not reliably protected — which is what anyone entrusting data to the company needs to know.

How it is evaluated: see LC3 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: GDPR Art. 83; FTC Privacy Enforcement; Australia Privacy Act 1988 (OAIC); Japan APPI and Personal Information Protection Commission (PPC) enforcement actions; UK Information Commissioner's Office (ICO); France CNIL; EU European Data Protection Board (EDPB). The US$5 million floor for a single severe matter matches LC4 and is an xGTT policy choice, not drawn from a single source.

LC4. No Adjudicated IP Infringement

What it checks: Whether a court has found that the company willfully infringed intellectual property on a large scale — for example, copying protected works or inventions for a product it sells — within the look-back period. Ordinary disputes and settlements without a finding do not count.

Why: Deliberate, large-scale taking of others' intellectual property shows disregard for rights that democracies protect. Good-faith disputes are a normal part of business and are not counted.

How it is evaluated: see LC4 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: WIPO Copyright Treaty; US Copyright Act (17 U.S.C.); EU Copyright Directive 2019/790; UK Copyright, Designs and Patents Act 1988. The willfulness test follows US enhanced-damages practice (35 U.S.C. § 284) and findings of deliberate copying elsewhere; the US$5 million large-scale floor is an xGTT policy choice.

Background for LC1–LC4: Subsidiary attribution: the Standard's test for counting a subsidiary's finding against its parent follows the US DOJ and SEC FCPA Resource Guide, which looks at the parent's control — its knowledge and direction of the subsidiary's actions — not ownership percentage alone. Remediation: applying one remediation test across all four criteria mirrors the UK Serious Fraud Office's DPA Code of Practice, which covers bribery, fraud and money laundering under one framework, and US DOJ guidance on monitors and corporate compliance programs, written to apply across enforcement areas. Incident significance: xGTT's distinction between incidents that are disclosed and credited and incidents that count follows how regulators already weigh incidents. Under the GDPR, notifying a breach on time (Arts. 33–34) is a duty met, not a penalty,

© 2026 Krach Institute for Tech Diplomacy at Purdue

and a fine weighs gravity, intent, mitigation, the data affected, cooperation and prior infringements (Art. 83(2)); the NIS2 Directive (Art. 23) likewise sets staged reporting duties whose timely performance is expected. So a timely, complete disclosure of an incident exposing only contact-type data is credited, while a missed duty, sensitive data exposed at scale or a repeat pattern counts.

Transparency & Disclosures

Four criteria about what the company publicly discloses: audited accounts, how it handles government demands for data, how it manages its supply chain, and its anti-corruption, human-rights and whistleblower policies.

TA1. Independent Financial Audit

What it checks: Whether independent auditors have audited the company's financial statements and the audit opinion is public.

Why: Audited accounts are the baseline evidence that a company is what it says it is. Listed companies must publish them; privately held companies can do so voluntarily.

How it is evaluated: see TA1 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: PCAOB Audit Standards; IAASB International Standards on Auditing; EU Audit Directive 2014/56; UK Financial Reporting Council (FRC); Germany APAS; France H2A; India NFRA.

TA2. Government Data Request Transparency

What it checks: For companies that hold customer data, such as cloud, software-as-a-service and telecom providers: whether the company publicly commits to hand data to a government only when legally compelled, and to assess demands from governments rated Not Free, or formally identified as an adversary, against human-rights standards and challenge or refuse those that conflict with them.

Why: Customers entrust data to providers that operate in many countries. The test follows the norm that companies headquartered in democracies already apply in less-free markets, as set out in the Global Network Initiative principles: comply with lawful demands, but scrutinize demands from repressive governments.

How it is evaluated: see TA2 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: EU Digital Services Act Art. 24; Japan APPI Art. 24; South Korea PIPA Art. 18; Australia Telecommunications (Interception and Access) Act; US Stored Communications Act (18 U.S.C. §§ 2701-2712, the statute setting what legal process is required for each type of data — the standard the base-minimum test asks an entity to commit to); EU Charter of Fundamental Rights Art. 7-8 (the underlying legal-process principle CSPs cite in publishing law-enforcement-request guidelines); Global Network Initiative Principles and Implementation Guidelines, and the UN Guiding Principles on Business and Human Rights (the human-rights safeguard for demands from authoritarian governments); US DOJ Data Security Program, 28 CFR Part 202 (prohibitions on data access by countries of concern).

TA3. Democratic Supply Chain Conduct

What it checks: Whether the company avoids depending on suppliers that democratic governments have barred for national-security or forced-labor reasons, and publishes a supply-chain policy covering forced labor, human-rights due diligence, supplier rules, minerals sourcing where relevant, and a way to raise complaints.

Why: A company's trustworthiness extends to its suppliers. The policy checklist is drawn from what reference-country supply-chain laws and government procurement commonly require.

How it is evaluated: see TA3 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: EU Corporate Sustainability Due Diligence Directive (CSDDD); UK Modern Slavery Act 2015; US Uyghur Forced Labor Prevention Act (UFLPA); UN Guiding Principles on Business and Human Rights; OECD Guidelines for Multinational Enterprises; Germany LkSG; France Duty of Vigilance Law 2017; Norway Transparency Act 2022; Australia Modern Slavery Act 2018; Canada Fighting Against Forced Labour and Child

© 2026 Krach Institute for Tech Diplomacy at Purdue

Labour in Supply Chains Act; US Dodd-Frank Act §1502 and EU Conflict Minerals Regulation 2017/821 (conflict-minerals disclosure prong); US FCC Covered List (47 CFR 1.50002), the UK designated-vendor regime under the Telecommunications (Security) Act 2021, the US BIS Entity List and national high-risk-vendor regimes (restricted-vendor dependency test).

TA4. Anti-Corruption, Human Rights and Whistleblower Disclosures

What it checks: Whether the company publishes anti-corruption, human-rights and whistleblower policies that are working programs rather than boilerplate: named accountability, concrete procedures, a dated history and an applied recognized standard.

Why: These policies are how a company commits publicly to behave well and lets insiders report when it does not. The quality test separates working programs from pledges.

How it is evaluated: see TA4 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: OECD Anti-Bribery Convention; UK Bribery Act 2010; UN Guiding Principles on Business & Human Rights; EU Whistleblower Directive 2019/1937; Germany Hinweisgeberschutzgesetz (HinSchG); Netherlands House for Whistleblowers.

Technical Security Practices

Eleven criteria about the company's security and technology practices. Several apply only to certain companies, such as AI developers or companies with physical operations; for others the result is N/A.

TS1. Cybersecurity Certification

What it checks: Whether the company holds a current, independently verified cybersecurity certification, such as ISO/IEC 27001, a SOC 2 report or an independently assessed NIST CSF 2.0 conformance profile, covering the operations evaluated. Self-declared conformance without independent review does not count.

Why: Independent certification is how democratic governments and large buyers check a supplier's security without auditing it themselves.

How it is evaluated: see TS1 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: ISO/IEC 27001:2022; NIST CSF 2.0; SOC 2 (AICPA); Australian Signals Directorate (ASD) Information Security Manual (ISM) and Essential Eight; UK NCSC; Germany BSI; Japan NISC; EU ENISA.

TS2. Public Vulnerability Disclosure Program

What it checks: Whether the company has a public way for outside researchers to report security vulnerabilities, such as a disclosure policy or bug bounty program.

Why: Vulnerabilities that outsiders find get fixed only if there is a channel to report them. Governments now expect one from their suppliers.

How it is evaluated: see TS2 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: ISO/IEC 29147:2018; CISA Binding Operational Directive 20-01; EU NIS2 Directive Art. 23.

TS3. Published Privacy Policy

What it checks: Whether the company publishes a privacy policy that tells people what data it collects, why, what their rights are, how long data is kept and whom to contact.

Why: Privacy laws across the xGTT democracies require these disclosures. A policy that covers them is the minimum for informed use.

How it is evaluated: see TS3 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: GDPR Arts. 13-14; CCPA/CPRA; Japan APPI; South Korea PIPA; France CNIL; Estonia AKI.

© 2026 Krach Institute for Tech Diplomacy at Purdue

TS4. Responsible AI and Technology Principles

What it checks: For companies with AI products or services: whether the company publishes responsible-AI principles that are a working program rather than boilerplate: named accountability, concrete controls, a dated history and an applied recognized framework. Principles do not qualify where a serious incident involving the company's AI products or services has not been remediated.

Why: AI systems can cause harm that users cannot see. Published, working governance is how a company shows it manages that risk. The test is the same whatever the framework permits, and for open or closed models.

How it is evaluated: see TS4 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: OECD AI Principles; EU AI Act; NIST AI Risk Management Framework; G7 Hiroshima AI Process.

TS5. Weapons- and Mass-Surveillance-Relevant AI Practices (sector-gated, additive to TS4)

What it checks: For companies that themselves sell or deploy autonomous weapons, autonomous targeting or population-scale surveillance AI: whether humans stay in control, including the ability to switch a fielded system off, and whether surveillance systems are under the oversight the applicable law requires. Judged on the company's record, not its policy alone.

Why: These are the uses where AI failures cost lives or liberty. The benchmark is the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, endorsed across democracies.

How it is evaluated: see TS5 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy (primary, cross-jurisdiction benchmark). Named national directives, illustrative only, read alongside it rather than in place of it: US DoD/DoW Directive 3000.09; UK JSP 936 (Defence AI doctrine); Japan Ministry of Defense AI guidelines (Sept. 2025). Not qualifying anchors for this criterion: EU AI Act (Art. 2 excludes military/defense use); NATO Principles of Responsible Use (does not name human control).

TS6. Export Compliance

What it checks: For companies whose products are subject to export controls: whether the company can show a working export-compliance program, through independent verification or a substantive published policy. Actual violations are assessed under RL2 and RL8.

Why: RL2 asks whether a government has established a violation; TS6 asks whether the company can show a working program. Keeping them apart avoids counting one fact twice.

How it is evaluated: see TS6 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: US Export Administration Regulations (EAR); Wassenaar Arrangement; EU Dual-Use Regulation 2021/821; UK Export Control Act 2002; Japan METI export control; Netherlands CDIU.

TS7. Environmental Compliance

What it checks: For companies with physical operations such as factories, data centers, energy generation, materials operations, or logistics: whether they run a documented environmental-management program and have no serious environmental enforcement left unaddressed.

Why: Physical operations carry environmental risks that regulators in every xGTT democracy police. A managed program is the accepted evidence that those risks are under control.

How it is evaluated: see TS7 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: ISO 14001:2015; EU Corporate Sustainability Reporting Directive (CSRD); US EPA ECHO; EU Industrial Emissions Directive.

TS8. Operational Resilience

© 2026 Krach Institute for Tech Diplomacy at Purdue

What it checks: Whether the company has documented business-continuity and incident-response capabilities, through a certification or a substantive policy, and no serious operational failure left unaddressed.

Why: Customers and governments depend on suppliers to keep running through crises. Resilience frameworks across the democracies require planning and timely incident reporting.

How it is evaluated: see TS8 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: NIST CSF 2.0; EU NIS2 Directive; ISO 22301; UK NPSA; Germany KRITIS-Dachgesetz; Netherlands Wwke (NCTV); Denmark CER Act (DEMA). The Standard's test for a critical operational failure is grounded in the structural pattern used across these frameworks: the EU's DORA (Regulation (EU) 2022/2554, Art. 18, with materiality thresholds set by Delegated Regulation (EU) 2024/1772) tests multiple defined criteria in combination rather than a single number; the U.S. federal banking agencies' 2021 Computer-Security Incident Notification Rule and the SEC's cybersecurity disclosure rules use a qualitative "materially disrupts a material portion of its customer base" standard rather than a bright-line threshold. Neither model converges on one number; both converge on multiple defined triggers assessed together, which is the pattern the Standard's test follows.

TS9. Secure Software Development

What it checks: Whether the company develops software securely — for example, producing software bills of materials and managing vulnerabilities — or publishes a substantive secure-development policy.

Why: Many major cyberattacks entered through insecure software supply chains. Democracies now require suppliers to show how they build and patch software.

How it is evaluated: see TS9 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: NIST Secure Software Development Framework (SP 800-218); EU Cyber Resilience Act; US Executive Order 14028; ISO/IEC 27034; France SecNumCloud (ANSSI); India CERT-In Secure Guidelines.

TS10. Frontier AI Risk Framework

What it checks: For frontier AI developers only: whether the company actually applies a process to test models before release and manage misuse risk, shown in at least one real decision rather than only a published policy.

Why: The most capable AI models can create serious risks. Laws and commitments in the xGTT democracies expect developers to test for and manage those risks before release.

How it is evaluated: see TS10 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: EU AI Act Arts. 51-55 (Art. 51's 10^25 FLOP threshold for general-purpose AI systemic-risk classification is the source for the recognized regulatory compute threshold in the Standard's definition of a frontier AI developer, used for TS10 and, with its proprietary-weights condition, TS11); GPAI Code of Practice; Seoul Frontier AI Safety Commitments; California SB 53; New York RAISE Act.

TS11. AI Model Weight and Algorithmic Security

What it checks: For companies that develop or control proprietary frontier model weights: whether the company protects its model weights under a recognized security framework at a risk tier supported by the models' disclosed capabilities, meets any legal duty to publish its safety and security approach, and has no unremediated confirmed unauthorized leak of model weights.

Why: Stolen frontier model weights would hand their full capability to whoever takes them, including hostile states. Protecting them is a security matter for everyone, not only the developer.

How it is evaluated: see TS11 in the xGTT Standard, which sets out what the company is expected to demonstrate. Section 08 (Criteria Rules) of the Methodology Guide sets out how the verdict is reached.

Anchors: RAND Corporation (Securing AI Model Weights; Achieving AI Model Weight Security Level 3, RR-A4704-1); Frontier AI Safety Commitments (AI Seoul Summit, 2024); California SB 53 (Transparency in Frontier Artificial Intelligence Act); EU AI Act Art. 55(1)(d); FedRAMP High Authorization to Operate; NATO NCIA certification records; US Center for AI Standards and Innovation (CAISI).

© 2026 Krach Institute for Tech Diplomacy at Purdue

Selected Glossary and References

Criteria Provenance
The companion document that explains the laws, government lists, international standards and established practices behind each xGTT criterion.

Critical and Emerging Technology (CET) Sectors
The 15 technology sectors to which xGTT applies: Advanced Communications & Networking; Advanced Computing; Advanced Manufacturing & Materials; Artificial Intelligence; Autonomous Systems & Robotics; Biotechnology; Cybersecurity & Data Security; Directed Energy; Energy Technologies; Human-Machine Interfaces & Neurotech; Hypersonics; Positioning, Navigation & Timing; Quantum Technologies; Semiconductors & Microelectronics; and Space Technologies.

Deferred Prosecution Agreement (DPA)
An agreement under which a prosecutor suspends criminal charges in exchange for conditions such as penalties, cooperation and compliance reforms.

Entity List
A list maintained by the US Department of Commerce's Bureau of Industry and Security of foreign parties subject to special licensing requirements for exports of controlled items.

FedRAMP
The US Federal Risk and Authorization Management Program, which standardizes security assessment and authorization of cloud services used by federal agencies.

Finding
The result of the research an evaluator carries out on the public record, such as an entry found on a sanctions list or a policy found on a company website. Findings support verdicts. A decision by a government, regulator or court is called a government, regulatory or court finding.

Frontier AI Developer
A company that develops general-purpose AI models at or near the leading edge of capability, identified by its own description or by a recognized regulatory compute threshold.

Global Network Initiative (GNI)
A multi-stakeholder initiative whose principles guide how technology companies respond to government demands that may affect privacy and freedom of expression.

Home Country
The country in which a company is legally incorporated or has its registered seat.

ISO 14001
An international standard specifying requirements for an environmental management system.

ISO 22301
An international standard specifying requirements for a business continuity management system.

ISO/IEC 27001
An international standard specifying requirements for an information security management system, against which organizations may be independently certified.

Methodology Guide
The companion document that sets out how an evaluator applies the xGTT criteria to a company using public evidence, including how an AI-prepared draft report is produced and what the person reviewing it must check.

© 2026 Krach Institute for Tech Diplomacy at Purdue

N/A
Not Applicable. The verdict recorded when a criterion does not apply to a company's sector or business model.

NIST
The US National Institute of Standards and Technology, a federal agency within the US Department of Commerce that develops standards, measurements, and technology guidance.

Not Free
The lowest of the three ratings (Free, Partly Free, Not Free) that Freedom House gives countries for political rights and civil liberties in its annual *Freedom in the World* report.

OFAC SDN List
The Specially Designated Nationals and Blocked Persons List maintained by the US Treasury's Office of Foreign Assets Control.

PASS and FAIL
Verdicts recorded when a criterion's conditions are met (PASS) or its failure conditions are established (FAIL).

Policy Quality Test
A published policy counts as a working program when it meets at least three of four indicators: the policy (1) names an accountable person or body; (2) describes concrete controls, processes or metrics; (3) is dated or versioned, or an earlier copy is accessible; and (4) names a recognized standard and explains how that standard is applied to the company's operations. Two indicators leave the criterion UNCLEAR. Zero or one is a FAIL, and so is a required policy that cannot be found after a complete search.

Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy
A declaration endorsed by democratic governments setting norms for the military use of AI, including human control and the ability to disengage systems.

Red-Line Criteria
The ten criteria checked before the Four Dimensions of Trust are evaluated. A FAIL on any one disqualifies the company; an UNCLEAR verdict does not.

SOC 2
A report under American Institute of Certified Public Accountants (AICPA) standards on a service organization's controls for security, availability, processing integrity, confidentiality or privacy.

Software Bill of Materials (SBOM)
A machine-readable inventory of the components and dependencies in a piece of software. SPDX and CycloneDX are standard SBOM formats.

UN Guiding Principles on Business and Human Rights (UNGPs)
The UN framework setting out the corporate responsibility to respect human rights, including through human-rights due diligence.

UNCLEAR
The verdict recorded when the available public evidence does not settle a criterion. It is not a negative verdict.

Verdict
The label each criterion receives in an evaluation report: PASS, FAIL, UNCLEAR or N/A. Verdicts are never combined into an overall score or rating.

xGTT Democracies
The 18 technologically advanced democracies whose laws and practices ground the xGTT criteria: Australia, Canada, Denmark, Estonia, Finland, France, Germany, India, Israel, Japan, Netherlands, New Zealand, South Korea, Sweden, Switzerland, Taiwan, the United Kingdom, and the United States.

© 2026 Krach Institute for Tech Diplomacy at Purdue

Closing Notice

The Global Trusted Tech Standard (xGTT) is an open standard published by the Krach Institute for Tech Diplomacy at Purdue (the “Krach Institute”). Use of xGTT is subject to the xGTT Terms of Use available from the Krach Institute and your use of xGTT shall constitute your acceptance of those terms of use. The Krach Institute and affiliated entities disclaim all liability from the use of xGTT and users are advised to follow the standards for fact-based evaluations and may be subject to claims by third parties relating to your evaluation. No evaluation, rating, or score made using xGTT is a substitute for independent due diligence. Anyone considering a transaction or investment, or other decision involving an evaluated government, company, or organization should perform its own independent investigation and analysis and should not rely on any xGTT evaluation for that purpose.

© 2026 Krach Institute for Tech Diplomacy at Purdue

TechDiplomacy.org