PerilScope

СТРАТЕГИЧЕСКИ ХОРИЗОНТИ

Когато доверието изпреварва доказателствата

Тъмната страна на стандартизацията, акредитацията и сертификацията

Изкуственият интелект, геополитическата фрагментация и климатичният натиск променят както онова, което обществото очаква от системите за оценяване и удостоверяване, така и възможностите за злоупотреба с техния авторитет.



Иван Савов
Председател на ЕИРП — Европейски Институт за Риск Политика

Световен ден на стандартизацията · 14 октомври 2026 г.
Българско издание за професионално разпространение

Съдържание

Когато доверието изпреварва доказателствата

Обещанието и уязвимото място.....3

Как удостоверяването придобива повече авторитет, отколкото заслужава.....4

Какво показват доказателствата и какво не доказват.....5

Бизнесът с доверие.....7

Кой пише правилата и кой може да си позволи да ги изпълни?.....8

Доверие в разделен, но взаимосвързан свят.....9

ИИ навлиза в самия механизъм на доверието.....11

Цифрови доказателства, климатичен натиск и границите на валидния сертификат.....13

Сценарии: бъдещето на системата за доверие, 2026–2033 г.....15

Посоката напред: доверие, което издържа проверката на действителността.....18

За доклада и източниците.....20

Публичен аналитичен доклад. Информационен хоризонт: 14 октомври 2026 г. (Europe/Sofia).

Номерата в квадратни скоби отвеждат към съответните източници в края на документа. Историческите материали в източници [1]–[4] и [29] се съхраняват в Архива на ЕИРП (ERPI Archive).

Обещанието и уязвимото място

Сертификатът е обещание, събрано в документ. Той казва на купувача, регулатора, инвеститора или гражданина, че компетентна страна е проверила нещо важно спрямо договорено изискване. Съвременните икономики зависят от това обещание. Малцина могат лично да проверят фабриките, които произвеждат лекарствата им, да повторят изпитванията на строителните материали или да проучат всяка организация, която обработва данните им. Стандартите и оценяването на съответствието позволяват да вземаме решения отвъд границите на собственото си пряко познание.

Опасността започва, когато обещанието надхвърли доказателствата. Сертификатът за система за управление се превръща в твърдение, че всеки продукт е безопасен. Лабораторният резултат става гаранция за цяла верига на доставки. Акредитацията се възприема като доказателство, че нарушения са невъзможни. Вписването в база данни замества въпроса дали самото оценяване е било компетентно, независимо и относимо към конкретния случай. Ограниченото удостоверяване се превръща в неограничено доверие.

Именно тази уязвимост разглежда докладът. Измамата я използва, но не я обяснява изцяло. Автентични документи могат да съдържат необосновани оценки. Надеждни оценки могат да бъдат прилагани извън своя обхват. Технически верни констатации могат да подкрепят подвеждащи твърдения. Доказателствата могат да остареят, докато институционалният им авторитет остава непокътнат. Затова най-тежкият провал може да пристигне с валиден документ и разпознаваемо лого.

През септември 2014 г. подготвих презентацията „Conformity Assessment in Gotham City“ с подзаглавие „The Dark Side of Standards, Accreditation and Certification“ за среща на ISO/CASCO в Женева. Тя разглеждаше пресечната точка между корупцията, подкупите, фалшифицирането и институциите, които трябва да правят търговията надеждна. През 2015 г. работата ми разшири този анализ към мрежите: документите, стоките, посредниците и паричните потоци трябваше да бъдат изследвани заедно. Основният въпрос остана: как една система, създадена да поражда доверие, предотвратява превръщането на това доверие в средство за измама? [1]

Дванадесет години по-късно въпросът има по-широки измерения. Изпитването, контролът и сертификацията — секторът TIC, от английското Testing, Inspection and Certification — навлизат в управлението на изкуствения интелект, екологичните твърдения, цифровите вериги на доставки и стратегическата индустриална политика. Акредитацията придобива по-голямо значение за обществените решения точно когато условията за надеждно оценяване стават по-трудни за поддържане. Едни и същи институции трябва да се справят с търговски натиск, техническа сложност, геополитическо разделение и физически смущения.

Отправната точка са по-ранните анализи на PerilScope за веригата на доверие и променящия се TIC сектор. Този сектор все повече отговаря за доказателства, които трябва да издържат на проверка в различни организации, юрисдикции и моменти във времето. Геополитическите анализи на Chancellor добавят важен извод: жизненоважни връзки могат да продължат да функционират, докато капацитетът, който ги поддържа, се изчерпва. В системата за оценяване и удостоверяване това означава, че нарастващият брой сертификати може да съществува едновременно с отслабен технически контрол, претоварени оценители или ограничен достъп до първични доказателства. Активността и устойчивостта са различни показатели. [3] [4]

Световният ден на стандартизацията е подходящ повод да разгледаме това напрежение. Фокусът му през 2026 г. върху достъпната и чиста енергия прави връзката особено конкретна: оборудването, инфраструктурата, твърденията за емисии и системите за тяхната проверка се нуждаят от достоверни доказателства. Следващият анализ защитава тази обществена функция чрез критично изследване на нейните уязвимости. Целта му е да установи как доверието може да остане заслужено в свят, който ще изисква все повече от него. [30]

Как удостоверяването придобива повече авторитет, отколкото заслужава

За читателите извън професионалната общност са важни няколко разграничения. Стандартът определя изисквания, методи или съгласувани практики. Оценяването на съответствието проверява дали определени изисквания са изпълнени. Изпитването осигурява доказателства за конкретни характеристики при посочени условия; контролът оценява обект, процес или инсталация; сертификацията представлява удостоверяване от трета страна в рамките на определена схема. Акредитацията оценява компетентността и безпристрастността на органите, извършващи конкретни дейности по оценяване на съответствието. Споразуменията за признаване улесняват приемането на резултатите през границите. Тези функции взаимно се подкрепят, но никоя не дава неограничена гаранция.

Одитът на система за управление и изпитването за безопасност на продукт отговарят на различни въпроси. Същото важи за верификацията на отчетени въглеродни емисии и оценката дали заявена екологична полза би настъпила и без съответния проект. Смесването на тези категории придава на ограничен извод привидна универсална валидност. Обществото обикновено вижда крайния знак или сертификат; уговорките, ограниченията на извадката, изключените обекти и техническите допускания остават далеч по-незабележими.

Оттук следват пет различни механизма на провал. Първият е фалшифицирането: неистински сертификат, измислен издател или подправен резултат. Вторият е некачественото оценяване: реален доставчик издава автентичен документ след недостатъчна или недобросъвестна работа. Третият е неадекватността на критериите: методът се прилага правилно, но не доказва резултата, който обществото смята, че доказва. Четвъртият е неправомерното разширяване на обхвата: оценка на една организация, обект, конфигурация на продукт или управленски процес се пренася върху нещо друго. Петият е загубата на актуалност: условията на дейност се променят достатъчно, за да отслабят значението на предходната констатация.

Тези разграничения имат пряко практическо значение. Регистърът с възможност за търсене може да помогне за откриването на измислен сертификат. Той не може да докаже, че пропуснатото посещение на място е било извършено. По-доброто обучение на одиторите може да подобри оценяването, но не може да поправи методология, която измерва погрешното нещо. По-надеждният метод не предотвратява преувеличените рекламни послания, ако самото твърдение не бъде оспорено. По-навременният надзор може да установи промяна в условията, ако системата разпознава кога е необходимо ново оценяване. Неподходящото решение може просто да създаде по-сложна версия на първоначалната слабост.

Във веригата участват и онези, които се доверяват на удостоверяването. Отделът по снабдяване може да изисква сертификат главно защото той лесно се превръща в критерий

за оценка. Инвеститорът може да използва знак, за да опрости сложна преценка. Регулаторът може да възложи техническата работа на други, без да запази достатъчен капацитет да я поставя под въпрос. Когато приемащата институция третира удостоверението като самото решение, вместо като доказателство в негова подкрепа, отговорността се размива. Всеки може да посочи спазена процедура, без никой да е установил дали изводът за действителността е обоснован.

Това не обезсмисля оценяването и удостоверяването. Извадките, професионалната преценка и изводите с ограничен обхват са неизбежни в сложните системи. Въпросът е дали ограниченията остават видими и дали противоречащите доказателства могат да променят решението. Надеждната система прави повече от това да издава положително становище. Тя може да го ограничи, откаже, временно спре или оттегли и да осигури достигането на корекцията до онези, които са разчитали на него.

Събраните за този доклад доказателства не позволяват да бъде посочен защитим глобален процент на измамите при сертификацията. Оценките за търговията с фалшифицирани стоки често се използват неправомерно за запълване на тази празнина. Проучването на ОИСР и EUIPO от 2025 г. оценява международната търговия с фалшифицирани и пиратски стоки на до 467 млрд. щатски долара, или 2,3% от световния внос, въз основа на данни за 2021 г. Това е оценка с определен обхват на друго явление, а не измерване на измамната сертификация през 2026 г. Механизмите заслужават сериозно внимание и без изкуствено произведено число за заглавието. [10]

Какво показват доказателствата и какво не доказват

Най-силният аргумент за критичен анализ идва от документирани провали в различни системи. Тези случаи не бива да се сливат в едно общо обвинение срещу акредитацията. Те засягат различни правни режими, дейности по оценяване и доказателствени резултати. Разгледани заедно, показват как системите за удостоверяване могат да се провалят на повече от едно равнище, включително в утвърдени институции със значителни технически ресурси.

Когато надзорът става прекалено снизходителен

Докладът от втората фаза на публичното разследване за Grenfell Tower е особено важен, защото подробно изследва отношенията между продуктите, сертификацията и надзора. При разглеждането на надзора на United Kingdom Accreditation Service върху British Board of Agrément и Building Research Establishment разследването установява сериозни слабости, включително недостатъчна задълбоченост на проверките и неспособност да бъде постигнато ефективно подобрение. Това са констатации на публично разследване; те не бива да се представят като наказателни присъди. Значението им надхвърля Великобритания: надзорът може да установява недостатъци, без да доказва, че основният проблем е отстранен. [5]

Изводът е неудобен. Формалното пренасяне на проблема към по-високо равнище не означава непременно ефективна намеса. Повтарящите се уверения за предприети коригиращи действия могат да запазят административната непрекъснатост, докато същностната слабост остава. Решаващият въпрос е дали надзорът може независимо да провери поведението и резултатите, вместо да разчита на разказа на организацията за собственото ѝ подобрение.

Реални издатели, ненадеждна работа

През септември 2026 г. китайската Държавна администрация за регулиране на пазара — SAMR — публикува шест случая на нарушения при сертификацията на качеството. Те включват неверни одитни материали, пропусната работа на място, необосновано съкращаване на времето за одит и проблеми с обхвата или поддържането на продуктовата сертификация. Това са публикувани от регулатора административни констатации, а не представително изследване на китайския сертификационен пазар. Те показват и активност по прилагането на правилата. Би било аналитично погрешно по-голямата видимост на нарушенията автоматично да се приема за доказателство за по-ниска почтеност в дадена държава. [6]

По-общият урок е, че установяването на автентичността не решава всеки проблем. Автентичен издател може да произведе ненадежден резултат. Юридическото съществуване на организацията и наличието на валиден запис оставят отворен въпроса каква работа действително е извършена. Когато търговският натиск насърчава бързото издаване, най-важните доказателства могат да бъдат свързани с отделеното време, достъпа, извадката и правомощията на лицето, което взема техническото решение.

Изпитвания, записи и границите на последващото успокоение

Японското Министерство на земята, инфраструктурата, транспорта и туризма документира нарушения при изпитванията за одобряване на типа на автомобили Daihatsu и последващите проверки. Регулаторното одобряване на типа е различно от сертификацията на система за управление по ISO. Това разграничение е важно: последващо установяване, че автомобилът изпълнява техническо изискване, не доказва, че първоначалната процедура по одобряване е била честна или надеждна. Съответствието на продукта и почтеността на процеса са свързани въпроси, но изискват различни доказателства. [7]

В Съединените щати Министерството на правосъдието съобщава през януари 2024 г. за осъждането на двама мъже след признания за виновност по случай с фалшифицирани записи за калибриране на изпитвателно оборудване, използвано в атомни електроцентрали. Случаят установява престъпно поведение, свързано със записи; той не доказва авария на реактор, нито че всяка засегната дейност е извършена от акредитирана лаборатория. Стратегическият урок е възможният обхват на малък доказателствен провал: неверен запис може да се превърне във входна информация за решения, отдалечени от неговия източник. [8]

Продължаващото производство по случая „Брумадиньо“ в Бразилия показва залога на декларациите за безопасност в друга среда. Информацията на Федералната прокуратура от 2026 г. описва разпити и събиране на доказателства по висящо наказателно дело. Обвиненията трябва да останат обвинения, докато производството продължава. Случаят не позволява предварително произнасяне за вина, но подчертава обществения интерес към това как се изготвят, оспорват и използват технически декларации, когато последиците от провал са тежки. [9]

Тези примери не доказват, че всички системи за оценяване и удостоверяване се влошават. Повече случаи могат да означават по-добро разкриване, по-прозрачно правоприлагане или по-голям брой оценявани обекти. По-малко съобщени проблеми могат да означават по-добри резултати, по-тесен надзор или по-трудно достъпен механизъм за жалби. Доказателствата подкрепят изследването на механизмите и корекциите, но не дават отговор за глобалната разпространеност или основание за опростени класации по държави.

Бизнесът с доверие

Оценяването и удостоверяването функционират в пазарна среда. Обикновено оценяваната организация избира и заплаща доставчика, докато голяма част от ползата от строго, но неблагоприятно за нея решение се получава от клиентите, работещите и обществото. Това напрежение може да бъде управлявано, но не може да бъде премахнато с пожелания. Търговските и техническите правомощия трябва да бъдат достатъчно разграничени, за да може оценителят да каже „не“, когато „да“ би запазило приходите.

Компромисът не е задължително да започва с подкуп. Търгът възнаграждава най-краткия срок. Доставчикът намалява времето на специалистите. Местният партньор обещава безпроблемен резултат. Неудобна констатация се смекчава. Техническият проверяващ получава изгладено досие, от което е премахната несигурността, тревожила оценителя. Нито една отделна стъпка не изглежда решаваща, но общият им ефект може да бъде такъв. Именно затова по-ранната ми работа по избора на сертифициращ орган поставяше акцент върху юридическите и оперативните отношения зад марката. [2]

Една възможна последица е търсенето на по-удобен одитор, макар смяната на доставчик да може да бъде напълно основателна. Клиентът може да получи по-добра компетентност, обслужване или независимост чрез такава промяна. Проблемът възниква, когато прехвърлянето прикрива неблагоприятни констатации или позволява нерешени проблеми да изчезнат в новото договорно отношение. Същият въпрос важи за придобиванията и подизпълнението: следва ли съществената история съответната дейност, или промяната на име, договор или информационна система я заличава?

Престъпната злоупотреба също може да използва обичайни търговски отношения. Фалшивият документ е само една възможна входна точка. Посредник може да представи невярно кой е извършил работата; подменен продукт може да наследи репутацията на изпитания; мрежа от договори може да затрудни установяването на отговорността. Това са механизми за злоупотреба, а не обвинения срещу конкретна мрежа. Те обясняват защо акцентът от 2015 г. върху връзките между документи, стоки и посредници остава актуален: изследването само на удостоверението може да пропусне отношението, чрез което то придобива стойност.

Мащабът носи реални ползи. Голяма TIC група може да финансира специализирани лаборатории, техническо обучение, киберсигурност и международно покритие. Специализирана фирма може да притежава по-задълбочено местно или секторно познание. Собствеността и размерът сами по себе си не определят почтеността. Решаващо е дали техническото управление се развива със същото темпо като разрастването. По-лесно е да бъдат придобити лаборатории, отколкото да се осигури постоянна надеждност на техните методи, записи, контрол на достъпа и процедури за реакция при проблем.

Анализът на PerilScope „Evidence at Scale“ от февруари 2026 г. определя това като основен стратегически въпрос за сектора. Когато резултатите от изпитвания и записите от оценяване преминават през споделени цифрови системи, интеграцията се превръща във въпрос за целостта и достоверността на доказателствата. Общата платформа може да подобри съпоставимостта и проследимостта. Тя може също да разпространи конфигурационна грешка, слаб метод или компрометирани данни за достъп в много по-голяма мрежа. Ефективността и общите уязвимости могат да нарастват едновременно. [4]

Съществува и паралелна опасност от прекомерна сложност. Допълнителни схеми, многократни искания за документи и несъвместими изисквания на купувачите могат да погълнат оскъден инженерен и управленски капацитет, без да подобрят решението.

Малките предприятия може да изразходват по-голям дял от ресурсите си за доказване на съответствие в сравнение с големите конкуренти. Ако способна фирма бъде изключена, защото не може да финансира дублирана документация, системата не е избрала непременно по-безопасния доставчик.

Но опростяването изисква същата критичност като разширяването. Повторното използване на проверени данни за юридическо лице може да намали тежестта. Премахването на независима проверка на критична продуктова конфигурация може да отстрани точно момента, в който опасната подмяна би била разкрита. По-ниската цена може да отразява реална производителност или недостатъчно извършена работа; по-високата — специализирана компетентност или пазарна власт. Нито цената, нито обемът на документацията са надежден заместител на оценката за обществена полза.

Оценяването и удостоверяването в областта на ИИ изострят тези политико-икономически въпроси. Технологичните компании имат интерес да избягват забавяния и да запазят свободата си при внедряване. TIC доставчиците имат интерес от значим пазар за оценяване от трета страна. Регулаторите имат интерес от приложими правила и видим авторитет. Аргументите им могат едновременно да съдържат основателни технически съображения и търговски интерес. Обществената политика отслабва, когато предпочитаната от някой участник пазарна структура се представя като единствения възможен израз на безопасност. Това беше основна тема в по-ранния анализ на PerilScope за дебата около удостоверяването на ИИ. [29]

Кой пише правилата и кой може да си позволи да ги изпълни?

Тъмната страна може да се прояви още преди оценяването. Стандартите определят кои свойства имат значение, кои методи са приемливи и кои форми на доказателства се признават. Тези решения влияят върху инвестициите, достъпа до пазари и цената на иновациите. Едно изискване може да служи на основателна цел за безопасност и едновременно да облагодетелства технологии или организационни практики, познати на най-активните участници в неговото разработване.

Това не е достатъчно доказателство за завладяване на процеса от частни интереси. Техническият опит, зависимостта от предходни решения и реалните различия в риска могат да обяснят неравномерния резултат. Твърдението за такова завладяване е по-силно и изисква доказателства, че упражненото влияние е изкривило решението. Но и формалната отвореност не е пълен отговор. Организацията може да има право да участва, без да разполага с персонала, езиковата подкрепа, средствата за пътуване или времето, необходими за влияние върху технически сложен процес.

Принципите на Световната търговска организация за разработване на международни стандарти включват прозрачност, отвореност, безпристрастност и консенсус, ефективност и приложимост, съгласуваност и отчитане на потребностите на развитието. Значението им е във връзката между техническата легитимност и участието. Стандарт, който се прилага по света, не бива да предполага, че практическата възможност за влияние върху съдържанието му е разпределена равномерно. [11]

Докладът за световното развитие на Световната банка за 2025 г. разглежда стандартите като инструменти на развитието и подчертава прехода от приспособяване към тях, през привеждане в съответствие, до участие в създаването им. Това е важен коректив на разказ, съсредоточен единствено върху изключването. Стандартите могат да помогнат на фирмите да учат, да подобряват качеството и да навлизат на по-големи пазари, когато има

надеждна подкрепа за прилагането им. Проблемът е разминаването между изискването за доказателства и създаването на възможност те да бъдат произведени. [12]

Обновената трилогия на UNIDO за политиката по качеството, представена през април 2026 г., също поставя инфраструктурата по качеството в контекста на устойчивата индустриална и цифрова трансформация. Лабораториите, метрологията, подготвените оценители и ефективните институции са производствен капацитет, а не странични административни разходи. Държава, зависима от внесен отвън капацитет за оценяване, може формално да изпълнява изискванията и все пак да остава зависима от външни преценки за собственото си производство. [13]

Затова регионалните инициативи трябва да се разглеждат и като проява на самостоятелна способност за действие, наред с възможността да пораждат фрагментация. Африкански, азиатски, латиноамерикански и арабски институции могат да разработват подходи, съобразени със своите икономики, и да участват в международното създаване на правила. Континенталната стратегия на Африканския съюз за ИИ, одобрена през 2024 г., изрично свързва отговорното използване на ИИ с капацитета и участието. Съществуването ѝ не доказва изпълнение, но оспорва предположението, че останалият свят само избира между правила, създадени в Европа, Съединените щати или Китай. [24]

Достъпът има и правно измерение. През март 2024 г. Съдът на Европейския съюз се произнесе по дело C-588/21 P относно публичния достъп до хармонизирани стандарти за безопасност на играчките, като призна наличието на по-висш обществен интерес от оповестяване при разглежданите обстоятелства. Решението не отменя авторското право върху всички стандарти. То обаче разкрива основно напрежение, когато частно разработени изисквания придобиват правно действие: хората трябва да имат реална възможност да разбират и оспорват правилата, които ги обвързват. [14]

Общественият интерес е защитен, когато строгите изисквания са технически обосновани, разбираеми и изпълними по справедливи начини. Това включва финансиране на експертния капацитет за поддържане на стандартите. Включва и поставяне под въпрос на ненужни добавки, които създават зависимост от конкретни схеми, платформи или доставчици на услуги. Качеството на управлението се разкрива в баланса между тези интереси, а не в това дали създателят на правилата е публична или частна организация.

Доверие в разделен, но взаимосвързан свят

Геополитическият въпрос е по-дълбок от това дали държавите приемат един и същ стандарт. Общото изискване не води автоматично до приемане на едни и същи доказателства. Правителствата могат да отчитат собствеността на лабораторията, местонахождението на данните, риска от санкции, достъпа до технически записи или значението на продукта за сигурността. Доставчикът може да е технически компетентен и въпреки това да среща ограничения на определен пазар. Обратно, политическата близост не доказва техническа надеждност.

Анализите на Chancellor очертават свят, в който съперничеството и избирателното сътрудничество съществуват едновременно. Държавите защитават някои връзки, защото икономиките и жизненоважните им услуги зависят от тях, дори когато ограничават други. За TIC сектора това означава многопластова среда: международно признаване в едни дейности, регионални или национални изисквания в други и правила на частни платформи, наложени върху двете. Техническото сътрудничество може да се запази без по-широко политическо сближаване.

Самата международна акредитационна система се промени. Global Accreditation Cooperation Incorporated, използваща наименованието Global ACI, започна пълноценно да функционира на 1 януари 2026 г. и пое предишните функции на IAF и ILAC. Публикуваните ѝ правила осигуряват приемственост чрез единна рамка за признаване и преходни условия за предходните знаци. Само логото не установява относимия обхват или статут, а международният преход не отменя националното законодателство. [15]

Обединяването създава възможност за намаляване на дублирането и по-добра координация. То увеличава и значението на институцията, чрез която се пренася доверието. Ако повече дейности зависят от обща рамка, информационна грешка, нерешен спор или неадекватна реакция на нарушение могат да имат по-широки последици. Институционалното обединение не води автоматично нито до по-добър надзор, нито до по-голяма уязвимост; резултатът зависи от начина, по който действат решенията, доказателствата и корекциите.

Global ACI публикува Кодекс за поведение със задължения за членовете и основания за дисциплинарни последици. Общественият въпрос е доколко последователно се прилагат тези задължения, как се разследват обоснованите сигнали и как ползвателите научават за съществени ограничения. Правилата са отправна точка за отчетността; доказаното им прилагане е по-силният тест. [16]

Надзорът зависи и от експертиза, която идва от самата общност, обект на надзор. Партньорското оценяване може да осигури задълбоченост, недостъпна за външни лица, но споделените професионални и институционални интереси могат да затруднят реакцията срещу неудобни констатации. Това е управленско напрежение, което трябва да бъде изследвано, а не доказателство, че партньорското оценяване е компрометирано. Институцията отслабва собствената си надеждност, когато опазването на доверието в системата получи предимство пред проверката дали то остава оправдано.

Геополитическата фрагментация може да затрудни тази проверка. Инспекторите могат да загубят достъп до обекти; техническите записи могат да бъдат ограничени; плащанията или придвижването на специализирано оборудване могат да бъдат възпрепятствани. Сертификатът може да остане видим, докато практическите отношения, поддържали надзора, отслабват. Когато под натиск се въвеждат алтернативни доставчици, може да се приеме, че доказателства за една конфигурация покриват друга. Това са условни механизми за пренасяне на риска, а не твърдения, че всяка санкционирана или оспорвана юрисдикция произвежда ненадеждни резултати.

Последиците действат и в обратна посока. Временно спиране, оспорен резултат от изпитване или отказ от признаване могат да засегнат снабдяването, митническото оформяне, финансирането и застраховането. Купувачите могат да реагират предпазливо спрямо цяла категория доставчици и да прехвърлят цената на несигурността върху фирми, които почти нямат отношение към първоначалния провал. Малките износители могат да понесат най-голямата тежест, защото разполагат с по-малко алтернативни пазари и по-ограничени средства за повторно оценяване.

И все пак оценяването и удостоверяването могат да останат мост през политическите разделения. Общи методи за изпитване, проследими измервания и достоверно установена еквивалентност могат да запазят полезно сътрудничество, без да изискват съгласие по всеки политически въпрос. По-силната стратегическа посока е избирателна оперативна съвместимост, подкрепена с доказателства: достатъчно обща основа за жизненоважния обмен и ясно признати ограничения. Това изисква повече от обявяването на всеобщо доверие или на неизбежно разделение.

ИИ навлиза в самия механизъм на доверието

Изкуственият интелект често се обсъжда като нов обект на сертификация. Това е само част от значението му. Той навлиза и в създаването, тълкуването и движението на доказателствата. Оценяваната организация може да използва ИИ за подготовка на документацията си. Оценителят може да използва ИИ за подбор на извадки или анализ на записи. Органът по акредитация може да използва ИИ за проверка на оценителя. След това платформа за покупки може чрез ИИ да реши дали полученото удостоверение е достатъчно. Рискове могат да възникнат от взаимодействието между тези приложения, дори всяко поотделно да изглежда разумно.

Възможностите са реални

Добре проектираните инструменти могат да помогнат на анализаторите да съпоставят големи масиви от доказателства, да откриват несъответстващи дати, да превеждат записи, да установяват необичайни закономерности и да насочват оскъдното експертно внимание към случаи, които заслужават проверка. Те могат да намалят повтарящата се работа и да улеснят намирането на съществена информация. За по-малките организации това може да подобри достъпа до експертиза, която преди е била скъпа или недостъпна. Ползата зависи от качеството на първичния материал, пригодността на задачата и възможността резултатът да бъде проверен.

Автоматизацията може да възстанови и връзки, изгубени между разпокъсани системи. Промяна в статута може да достигне по-бързо до купувача; повтарящ се дефект може да стане видим в различни обекти; разминаване между сертификат и твърдение при възлагане на поръчка може да бъде открито преди решението. Това са реалистични възможности. Те трябва да се оценяват според действителните резултати, включително фалшивите тревоги, пропуснатите проблеми и разхода за проверка на сигнала.

Убедителната документация поевтинява

Генеративният ИИ може да създава гладко написани политики, правдоподобни описания на коригиращи действия и вътрешно съгласувани записи, без да установява, че описаните дейности са се състояли. Профилът на NIST за генеративния ИИ посочва рисковете от конфабулации — генериране на невярно, но правдоподобно съдържание — и от нарушаване на достоверността на информацията. За оценяването това означава нарастващо разминаване между документалната убедителност и доказателствата за действителната дейност. Това е възможен механизъм на риск; наличните източници не установяват глобална честота на сертификационните измами, генерирани с ИИ. [18]

Проблемът надхвърля очевидното фалшифициране. Организация може добросъвестно да използва модел, да приеме измислен детайл и да го пренесе в следващи доклади. Резюме може да премахне съществена уговорка, защото тя изглежда второстепенна. При превод може да се изгуби техническо разграничение. Многократното редактиране може да направи досието по-свързано, но по-малко вярно на първоначалното наблюдение. Така изопачаването може да стане системно, без да е започнало като координиран престъпен план.

Дистанционното оценяване добавя друга възможна уязвимост. Синтетични изображения, гласове или записи могат да затруднят установяването на присъствие и произход. Визуално убедителното представяне на процес не е равнозначно на наблюдение на процеса при условия, контролирани от оценителя. Отговорът не може да бъде всеобщ

отказ от дистанционна работа, която може да е необходима и ефективна. Методът за събиране на доказателства трябва да съответства на последиците от погрешен извод.

Кръгово потвърждаване и общи слепи петна

Нека разгледаме примерна верига. ИИ на доставчика създава досие за съответствие. ИИ на одитора го проверява спрямо изискване. Надзорен инструмент обобщава одита, а платформата на купувача превръща резултата в сигнал за одобрение. Ако инструментите използват сходни обучителни материали, шаблони или допускания, съвпадението между изводите им може да добавя твърде малко независимост. Четири резултата могат да повтарят една непроверена предпоставка.

Това е възможен механизъм на общ провал, а не установена констатация срещу конкретен доставчик. Значението му е в разликата между организационната обособеност и техническата независимост. Различни компании могат да зависят от едно семейство модели, облачна услуга, набор за сравнително оценяване или доставчик на данни. Общата грешка може да премине през последователни проверки точно защото при всяка от тях материалът изглежда познат и правдоподобен.

Тогава се променя и оскъдният ресурс. Създаването на приемливо изглеждащо досие става по-лесно, докато независимият досег с действителната работа остава труден. Първичните измервания, контролираните наблюдения, компетентно проведените интервюта и противоречащите доказателства придобиват по-голяма стойност. Особено уязвима ще бъде система, която възнаграждава привидната пълнота. Система, способна да поставя под въпрос собствените си предпоставки, има по-добър шанс да се усъвършенства.

Каналът за доказателства се превръща във възможност за атака

ИИ агенти, които четат документи и извършват действия, създават допълнителна категория уязвимост. Работата на NIST от януари 2026 г. по сигурността на агентни системи посочва рискове като непряко внедряване на злонамерени инструкции, умишлено замърсяване на данни и вредни действия, възможни дори без злонамерен вход. Документ може да съдържа материал, предназначен да пренасочи поведението на системата, която го анализира. Информация, която трябва да се третира като доказателство, може да бъде погрешно възприета като инструкция. [19]

В процеса на оценяване последицата може да варира от изкривено резюме до неразрешено разкриване на информация или неправомерна промяна на статут. Това са примерни последици, а не установени тук реални инциденти. Затова разликата между инструмент, който съветва оценителя, и инструмент, който може да промени регистър или да одобри доставчик, е основополагаща. По-голямата автономност променя възможния обхват на грешката и необходимия вид отчетност.

Традиционните киберрискове също остават актуални. Компрометирани данни за достъп, незащитени интерфейси или недостъпни облачни услуги могат да нарушат цифровата мрежа за удостоверяване независимо от способностите на моделите ѝ. Зависимостта от външни ИИ услуги поражда въпроси и за чувствителните промишлени данни, юрисдикцията, сроковете на съхранение и непрекъснатостта. Доставчикът може да запази юридическата отговорност, докато губи практическа видимост върху поведението на критичен компонент от собствения си процес на оценяване.

Оценяване на ИИ без преувеличаване на извода

Стандартизационната инфраструктура се развива. ISO/IEC 42001:2023 определя изисквания към система за управление на ИИ. ISO/IEC 42006:2025 добавя изисквания към органите, които одитират и сертифицират такива системи. Публичната програма на ANAB включва акредитация на органи за сертификация на системи за управление на ИИ. Това показва, че организационното управление и компетентността на оценителите са предмет на целенасочена работа. То не превръща сертификата за система за управление в доказателство, че всеки ИИ модел е безопасен, законосъобразен или надежден при всяко внедряване. [21] [22] [23]

Доказателствата трябва да съответстват на твърдението. Оценката на организационните механизми за контрол е различна от изпитването на конкретна версия на модел. И двете са различни от преценката за система, работеща с определени данни, инструменти, потребители и права за достъп. Моделът може да се промени след актуализация. Начинът на използване може да се промени, без да се променя самият модел. Приложение, което работи приемливо на един език или в една институционална среда, може да се държи различно в друга.

Международният доклад за безопасността на ИИ за 2026 г. посочва съществени ограничения на оценяването, включително разминавания между резултатите при сравнителни изпитвания и поведението при реално внедряване. За оценяването на съответствието това означава, че успешното изпитване трябва да запази ясно своите граници: изследваната система, условията, метода и онова, което резултатът не установява. Констатациите в доклада подкрепят внимателния подход към качеството на оценяването; те не означават, че всяко изпитване е безполезно. [20]

Човешкият надзор има сходни ограничения. Човек, който формално одобрява автоматизирана препоръка, не осигурява непременно независима преценка, ако няма достатъчно време, техническа компетентност или правомощия да я оспори. Обратно, отказът от полезни инструменти може да претовари експертите и да остави повече доказателства неизследвани. Съществено разграничение е между помощ, която укрепва професионалната преценка, и автоматизация, която оставя отговорността върху човек, вече неспособен реално да я упражнява.

Стратегическият риск е двупосочен: системата за оценяване може да сертифицира ИИ, докато става зависима от ИИ, който не разбира достатъчно. Възможността също е двупосочна. ИИ може да помогне за по-бързо откриване на несъответствия и зараждащи се провали, ако собственият му принос остава проследим и подлежащ на оспорване. Обществото трябва да може да разбере какво е оценено, каква роля е имала автоматизацията в решенията със значими последици и кой носи отговорност при оспорване на извода.

Цифрови доказателства, климатичен натиск и границите на валидния сертификат

Цифровата проверка адресира реална слабост: документът може да бъде копиран, променен или откъснат от своя издател. Регистрите и удостоверените записи затрудняват представянето под чужда самоличност и неразрешените промени. Те могат да свържат ползвателя с актуална информация и да намалят зависимостта от PDF, препратен през няколко посредници. Стойността им е значителна, при условие че изводът, направен въз основа на тях, остава точен.

IAF MD 28 въведе изисквания за въвеждане и поддържане на информация за сертификати на системи за управление, издадени под акредитация, в рамките на определения му обхват. Това е важно, защото проверката на статута става част от инфраструктурата, чрез която купувачите оценяват твърденията. Но регистърът не е всеобхватно преброяване на всички дейности по оценяване на съответствието. Липсващ запис изисква проверка на обхвата, изключенията и качеството на данните, преди да се прави извод за нарушение. Наличният запис установява регистриран статут, а не истинността на всяко допускане зад оценката. [17]

Цифровият подпис може да помогне за удостоверяване на изявление и за защитата му срещу определени промени. Той не може да направи невярното първоначално изявление вярно. Неизменяемият запис може да съхрани грешка толкова надеждно, колкото факт. По-честите актуализации могат да разпространяват остарели или неправилни тълкувания по-бързо, ако източникът е слаб. Затова цифровото доверие зависи от авторитета, качеството и възможността за корекция на първичните доказателства толкова, колкото от сигурността на записа.

Има и втора граница: времето. Подходът ERPI 3°C World Strategic Risk Policy® разглежда как институциите функционират при взаимосвързан физически, социален и геополитически натиск. Тук 3°C е условие за стратегическо планиране, а не твърдение, че такова затопляне вече е настъпило или ще настъпи навсякъде на определена дата. Въпросът е дали удостоверяването остава полезно, когато опасностите, зависимостите и способността за реакция се променят едновременно.

Горещините могат да повлияят на оборудването и условията на труд. Наводненията могат да прекъснат достъпа до обекти, записи и транспорт. Недостигът на вода или електроенергия може да компрометира производството и изпитванията. Извънредните покупки могат да въведат непознати доставчици и заместващи материали. Изложен на риск е и доставчикът на оценяване, а не само клиентът: лабораториите, инспекторите и цифровите регистри зависят от хора, инфраструктура и комуникации, които могат да бъдат натоварени едновременно.

Сертификатът може да остане формално валиден, докато условията, оправдаващи доверието в него, вече са се променили. Нека разгледаме хипотетичен критичен доставчик, чиято система за управление е оценена преди продължителен воден дефицит, спешно преместване на производството и смяна на ключов подизпълнител. Предишната констатация може да остане вярна в първоначалните си граници. Тя не установява, че новата конфигурация ще осигури същата непрекъснатост или резултати. Опасността е в непроверено разширяване на доверието от организацията, която се позовава на сертификата.

Съвместното комюнике на ISO и IAF от февруари 2024 г. въведе изрично разглеждане на относимостта на климатичните промени към контекста на системите за управление и изискванията на заинтересованите страни. Това е съществено развитие. То не представлява инженерно потвърждение за всеки актив, нито сертификация, че организацията може да издържи на определен сценарий на затопляне. Признаването на климатичната относимост и доказването на физическа устойчивост изискват различни доказателства. [25]

Екологичните твърдения разкриват сходен проблем. Директива (ЕС) 2024/825 изисква държавите членки да прилагат мерките за нейното изпълнение от 27 септември 2026 г. и урежда въпроси, свързани с маркировките за устойчивост, включително такива, които не се основават на отговарящи на изискванията сертификационни схеми или не са установени от публични органи. Правният обхват и националното прилагане имат

значение; това не е правило, че всички екологични твърдения изискват един универсален сертификат. По-широкият въпрос е дали формата на удостоверяване съответства на онова, в което обществото е приканено да вярва. [26]

Въглеродните кредити показват защо методологията изисква отделен анализ. През август 2024 г. Съветът за почтеност на доброволния въглероден пазар — ICVCM — отказа своя знак за висока почтеност на кредити по осем методологии за възобновяема енергия поради съмнения относно допълняемостта: дали ползата би възникнала и без съответния проект. По-късни решения през 2026 г. показват, че преработени подходи могат да бъдат разглеждани при определени условия. Това са решения за методологии в рамките на доброволно управление, а не констатации, че всеки засегнат кредит е свързан с престъпна измама. Добросъвестно верифицирана дейност може да не доказва заявената полза, ако методът е неадекватен. [27] [28]

Съвкупният риск е физическите смущения да увеличават потребността от бързи решения точно когато капацитетът за тяхната проверка отслабва. Повече документация може да замести липсващия достъп, специализираното време или независимото наблюдение. В обратната посока безразборното облекчаване на контрола може да допусне опасни заместители във вече натоварени системи. Стратегическото предизвикателство е да се запазят проверките, които имат значение, и същевременно да се освободи ресурс от работа, която допринася малко за качеството на решението.

Сценарии: бъдещето на системата за доверие, 2026–2033 г.

Следващите шест сценария адаптират по-ранната работа на ЕИРП за бъдещето на TIC сектора към разглежданите тук условия. Те са условни възможности за развитие, а не прогнози, оценки на вероятности или твърдения за намеренията на посочени институции. Разграничават сътрудничеството, капацитета, общественото доверие и контрола върху инфраструктурата на доказателствата. ИИ, климатичният натиск и геополитиката преминават през всичките шест: те са взаимодействащи сили, а не отделни сценарии.

Основният хоризонт е 2026–2033 г. По-дългосрочните последици се простират до 2040 г., когато решенията от настоящото десетилетие могат да са създали по-трайни институционални зависимости. Различни сценарии могат да се развиват едновременно в различни региони или сектори. Висококомпетентна лабораторна мрежа може да работи във фрагментиран пазар; ефективна международна рамка може да съществува редом със слабо местно прилагане.

1. Преплетена приемственост — повече отговорности, неравномерно обновяване (Braided Continuity)

Международното признаване остава полезно и до голяма степен запазено. Обединената акредитационна структура продължава да функционира, търсенето на цифрово и екологично удостоверяване нараства, а утвърдените TIC организации поемат нови дейности. ИИ подобрява част от рутинната работа, докато голяма част от системата продължава да зависи от периодично оценяване и човешка експертиза. Не настъпва решаващ институционален разрив.

Основното напрежение е дали капацитетът нараства толкова бързо, колкото отговорностите. Някои доставчици инвестират в методи, хора и сигурни данни. Други поддържат обема чрез съкращаване на оценяването, зависимост от шаблони или отлагане на интеграцията. Геополитическите ограничения се управляват чрез изключения и

допълнителни проверки. Климатичните смущения се поемат, но понякога чрез изчерпване на резерви от време на персонала и оперативна гъвкавост, които не се възстановяват.

Отличителни признаци биха били продължаващото трансгранично приемане на резултати наред с неравномерна задълбоченост на надзора, недостиг на специалисти и нарастваща дистанция между усъвършенстваните цифрови системи и по-слабото изпълнение в периферията. Противоположни доказателства биха били трайните подобрения на компетентността, коригирането и достъпа в цялата мрежа. Обществената последица е продължаващо доверяване на системата, но с все по-неравномерна защита зад привидно сходни удостоверения.

2. Единна и адаптивна система — капацитетът догонва търсенето (Unified Agile)

Международното сътрудничество става по-ефективно на практика. Регулатори, органи по акредитация и технически общности намаляват ненужното дублиране, като запазват строгото оценяване там, където последиците са най-значими. Цифровата инфраструктура свързва надеждна информация, а компетентни местни институции от повече региони участват в разработването на методите. ИИ помага за откриване на слаби доказателства и нововъзникващи закономерности, без да измества отговорността за решенията.

При този сценарий реформата се вижда в резултатите. Техническите корекции достигат по-бързо до ползвателите; преработени методи преодоляват известни ограничения; трансграничното приемане се улеснява, когато е доказана еквивалентност. Развитието на капацитет подобрява участието на по-малките фирми и икономиките с ограничени ресурси. Климатичните и киберсмущенията водят до работещо приспособяване, вместо до натрупване на постоянни изключения.

Основното препятствие е осигуряването на инвестиции и политическа ангажираност. По-добрата координация изисква ресурси и готовност да се разкрият слабости, които институциите може да предпочитат да решават незабелязано. Само по-бързото издаване на указания не би отличило този сценарий. По-силните сигнали са по-добри доказателства от реалната дейност, по-широко техническо участие и корекции, които намаляват повторяемостта на проблемите. Обществото получава едновременно по-надеждна защита и по-малка предотвратима административна тежест.

3. Тъкан под напрежение — системата се запазва, съдържанието изтънява (Stretched Fabric)

Формалните договорености оцеляват, но практическата им сила става неравномерна. Недостигът на компетентност, натискът за намаляване на разходите, разпокъсаното регулиране и повтарящите се извънредни ситуации правят надзора все по-неравномерен. Някои региони и сектори запазват задълбочен технически капацитет; други все повече зависят от дистанционни досиета, претоварени специалисти и евтини заместители. Признаването продължава да поражда доверие в мрежа, чието реално изпълнение става все по-непоследователно.

ИИ може както да прикрива това влошаване, така и да го облекчава. По-изгладените доклади и по-бързата обработка правят системата привидно продуктивна, докато все по-малко решения включват непосредствено изследване на сложни доказателства. Геополитическите ограничения стесняват сътрудничеството, а физическите смущения ограничават достъпа. Купувачите с повече ресурси закупуват допълнително удостоверяване; по-малките фирми и обществото разчитат на изтъняваща обща защита.

Възможни сигнали са повтарящи се неотстранени констатации, продължителни забавяния на експертните прегледи, повтарящи се извънредни изключения и трайно разминаване между отчетени корекции и наблюдавани резултати. Тези показатели изискват контекст: натрупването на чакащи случаи може да отразява нова, по-строга проверка, а не отслабнал капацитет. Определящият резултат е продължаваща институционална активност без съответно възстановяване на капацитета, който я оправдава.

4. Разрив в доверието — местен провал се превръща в системен шок (Fracture of Confidence)

Сериозен провал разкрива, че няколко равнища на удостоверяване са приели една и съща слаба предпоставка. Поводът може да бъде изпитване с критично значение за безопасността, екологично твърдение или процес на оценяване с участие на ИИ. При този хипотетичен сценарий вредата се разпространява, защото купувачите и регулаторите не могат бързо да определят кои резултати остават надеждни. Несигурността надхвърля пряко засегнатата организация.

Търсенето на повторно оценяване нараства точно когато техническият капацитет е най-ограничен. Доставчиците се сблъскват със забавяния, финансирането се затруднява, а някои институции се оттеглят към познати доставчици или национални доказателства. ИИ може да усили първоначалния провал чрез общи инструменти, но може и да помогне за определяне на засегнатия обхват. Решаващо е дали веригата на доказателствата може да бъде възстановена и границите на проблема — установени.

Този сценарий не предполага непременно траен срив. Прозрачното разследване и убедителната корекция могат да го насочат към обновяване. Защитните уверения, недостъпните записи и непоследователното третиране могат да го тласнат към фрагментация. Голям скандал сам по себе си не доказва системна криза; по-показателни биха били широко оттегляне на признаването, трайна неспособност да се разграничат надеждни от ненадеждни резултати и смущения при различни ползватели.

5. Паралелни системи на доверие — платформи и блокове се конкурират за авторитет (Parallel Trust)

Традиционната акредитация остава важна, особено в регулирани дейности и такива с критично значение за безопасността, но вече не определя всеки сигнал за надеждност, решаващ за търговията. Големи платформи непрекъснато оценяват информация за доставчици. Геополитически групировки обвързват достъпа до пазари със собствени правила, местонахождение на данните или одобрени доставчици. Фирмите работят в припокриващи се системи, които невинаги признават взаимно доказателствата си.

Платформените системи могат да предложат бързина, подробности за реалната дейност и полезна обратна връзка. Авторитетът им може също да стане труден за оспорване, когато една организация контролира пазара, данните и критериите за оценяване. Регионалните договорености могат да изградят необходим местен капацитет или да се превърнат в инструменти за изключване. Резултатът не може да бъде изведен само от това дали системата е частна, подкрепяна от държавата или международно призната.

Най-силните сигнали биха били решения при обществени и частни поръчки или регулиране, които придават самостоятелен авторитет на произведени от платформи доказателства; повтарящи се ограничения на достъпа до данни между системите; и растящи разходи за поддържане на няколко пътя за удостоверяване. Противотежест е натискът на ползвателите за преносимост, прозрачни критерии и независимо оспорване.

Обществената защита започва да зависи от възможността тези конкуриращи се системи да бъдат проверявани и свързвани, а не просто от скоростта, с която вземат решения.

6. Тъкан на доверието — желана посока, а не очаквана крайна точка (Trusted Weave)

Това е нормативният сценарий: бъдещето, което си струва да бъде преследвано. Оценяването и удостоверяването стават по-адаптивни, прозрачни и достъпни, без да обещават сигурност, която не могат да осигурят. Международното признаване запазва полезните връзки, регионалният капацитет дава реален глас на повече икономики, а цифровите системи улесняват проверката на произхода и ограниченията на важните твърдения.

ИИ подпомага техническата преценка, като остава под смислен надзор. Съществени промени в модели, условия на дейност или вериги на доставки могат да предизвикат преразглеждане на предходни изводи. Физическата устойчивост и непрекъснатостта се оценяват чрез ясно заявени допускания, вместо да се извеждат от неотносими сертификати. По-малки организации могат да получават достоверни доказателства, без да бъдат принуждавани да преминават през ненужни административни пластове.

Разликата спрямо „Единна и адаптивна система“ е в критерия за успех. Адаптивността се отнася до това колко бързо и компетентно институциите се приспособяват. „Тъкан на доверието“ поставя въпроса дали получената система разпределя справедливо защитата, възможността за участие и достъпа и дали остава отговорна пред хората, засегнати от решенията ѝ. Технологично развит пазар на удостоверяване може да изпълни първия критерий и да се провали по втория. Този път зависи от избори, ресурси и устойчив обществен контрол.

В шестте сценария най-показателното разграничение е между непрекъснатост, която обновява капацитета, и непрекъснатост, която го изчерпва. Броят на сертификатите, скоростта на цифровата платформа или наличието на споразумение за признаване сами по себе си не дават отговор. Доказателството е в това дали решенията остават технически защитими, дали корекциите достигат до ползвателите и дали хората запазват реалната възможност да поставят под въпрос упражнявания спрямо тях авторитет.

Посоката напред: доверие, което издържа проверката на действителността

Бъдещето на стандартите, акредитацията и сертификацията ще се определя от нарастващо търсене на доверие при условия, които правят заслужаването му по-трудно. TIC секторът навлиза все по-дълбоко във функционирането на икономиките, обществените политики и жизненоважните услуги. Значението му ще нараства с тази близост. Ще нараства и цената на допускането институционалният авторитет да надхвърля онова, което доказателствата могат да подкрепят.

Посоката е към оценяване и удостоверяване, които запазват връзката между твърдението, изследваните условия и вземаното решение. Автентичността е необходима, но е само един пласт. Компетентността, независимостта, адекватността на метода и запазената актуалност поемат останалата тежест. Система, достойна за доверие, трябва да може да обясни границите на изводите си, без да ги третира като търговска слабост.

ИИ прави тази дисциплина по-неотложна. Той може да разшири обхвата на експертизата и да разкрие слабости, които хората трудно забелязват в голям мащаб. Може също да умножи правдоподобните доказателства, общите слепи петна и решенията, чиято логика

нито едно отговорно лице не може да възстанови достатъчно добре. С навлизането на автоматизацията в механизма на удостоверяване независимостта трябва да се изследва през данните, моделите и инфраструктурата, а не само през организационните схеми. Човешката отговорност изисква реална способност за оспорване, а не само подпис в края на процеса.

Геополитическото разделение прави оперативната съвместимост едновременно по-ценна и по-оспорвана. Защитимата цел е да се запазят техническите връзки там, където доказателствата ги оправдават, при признаване на основателните правни различия и различията, свързани със сигурността. Климатичният натиск добавя изискването удостоверяването да остане смислено, когато условията на дейност се променят. И в двете области формалната непрекъснатост може да прикрива изчерпване; по-полезният критерий е дали работоспособният капацитет се поддържа и обновява.

Обществената легитимност зависи и от това кой участва и кой понася разходите. Свят, разделен между институции, които определят доверието, и икономики, които могат единствено да купуват достъп до него, ще остане уязвим. Способните регионални системи, компетентните местни специалисти и справедливите възможности за по-малките предприятия са част от качеството на глобалната система. Те разширяват и кръга от знания, с които могат да бъдат оспорвани слабите допускания.

Тъмната страна, очертана през 2014 г., се е разширила от злоупотреба със сертификати до по-широка борба за доказателства и авторитет. Отговорът е в институции, които желаят и могат да откриват неудобни факти, да преразглеждат преценките си и да правят последиците видими. Скандалите нанасят вреда, но система, неспособна да се коригира, е по-опасна от система, която разкрива собствените си провали.

В Световния ден на стандартизацията най-силната защита на стандартите е настояването техният авторитет да остава заслужен. Доверието е оправдано, когато доказателствата издържат на проверка, ограниченията им са разбрани и корекцията остава възможна. Бъдещето на системата ще зависи от способността ѝ да запази тази връзка, докато светът около нея става по-бърз, по-взаимосвързан и по-малко склонен да прощава грешките.

За доклада и източниците

Този публичен синтез се основава на презентационния архив на Иван Савов от 2014–2015 г., по-ранни публикации на PerilScope, работата на ЕИРП за бъдещето на TIC сектора и акредитацията и геополитическите анализи на Chancellor. Не включва препоръки към конкретни клиенти, вътрешни сценарни тегла или оперативни програми. Шестте сценария са адаптирани аналитични възможности; те не възпроизвеждат клиентска рамка за решения и не приписват прогнози на споменатите институции. Позоваванията на ANAB се отнасят до публичната му програма и не означават подкрепа за този доклад.

Информационен хоризонт: 14 октомври 2026 г., Europe/Sofia. Официалните констатации са отнесени към издалите ги органи; висящите производства са разграничени от съдебните решения. Аналитичните изводи и хипотетичните примери са обозначени в текста. Случаите илюстрират механизми и не са статистическа извадка. По-ранните публикации осигуряват идейна приемственост, а не независимо потвърждение на актуални факти. Подборът отчита различни регионални гледни точки и конкуриращи се обяснения. Не се твърдят глобален процент на измамите или вероятности на сценариите.

Автор: Иван Савов, председател на ЕИРП — Европейски Институт за Риск Политика. С изследователска и редакционна подкрепа от Aya (IAAI), партньор в съвместната интелектуална работа. ERPI 3°C World Strategic Risk Policy® служи като рамка за стратегическо разглеждане на системите под натиск; докладът не създава нов стандарт, сертификационна схема или институционален ангажимент.

© 2026 ЕИРП — Европейски Институт за Риск Политика / PerilScope. Всички права запазени.

Илюстрация: Ayo / PerilScope. Концептуално изображение, създадено с ИИ под човешко редакционно ръководство.

Източници

Историческите публикации са посочени като архивни материали, без връзки към премахнати публикации в LinkedIn. Останалите библиографски заглавия съдържат активни връзки към използваните източници.

[1] Иван Савов, презентации от 2014–2015 г. и свързана архивна публикация.
Архив на ЕИРП (ERPI Archive).
Бележка: отнасянето към ISO/CASCO в Женева е по спомен на автора, подкрепен от презентационните файлове от септември 2014 г.; независима програма на събитието не е намерена.

[2] Иван Савов, избор на сертифициращ орган, 14.11.2015 г.
Архив на ЕИРП (ERPI Archive).

[3] PerilScope, „The Chain of Trust — Public Synthesis“, 11.06.2026 г.
Архив на ЕИРП (ERPI Archive).

[4] PerilScope, „Evidence at Scale“, 14.02.2026 г.
Архив на ЕИРП (ERPI Archive).

[5] Grenfell Tower Inquiry, фаза 2, том 2, глава 28, 04.09.2024 г.

[6] SAMR, шест случая на нарушения при сертификацията, 18.09.2026 г.

[7] Япония, MLIT: нарушения при одобряване на типа на Daihatsu.

[8] САЩ, DOJ: присъди за фалшифицирани записи за калибриране, 25.01.2024 г.

[9] Бразилия, MPF: висящото наказателно дело „Брумадиньо“, 2026 г.

[10] ОИСР/EUIPO, „Mapping Global Trade in Fakes 2025“; данни за 2021 г.

[11] СТО, принципи за разработване на международни стандарти.

[12] Световна банка, „World Development Report 2025: Standards for Development“.

[13] UNIDO, обновена трилогия за политиката по качеството, 20.04.2026 г.

[14] Съд на ЕС, дело C-588/21 P, 05.03.2024 г.

[15] Global ACI, въпроси и отговори: функции, признаване и преход.

[16] Global ACI, Кодекс за поведение.

[17] IAF MD 28:2023 — въвеждане и поддържане на данни в базата на IAF.

[18] NIST AI 600-1, профил за генеративния ИИ, юли 2024 г.

[19] NIST/CAISI, сигурност на ИИ агентни системи, 12.01.2026 г.

[20] International AI Safety Report 2026, раздел 3.1.

[21] ISO/IEC 42001:2023 — системи за управление на ИИ.

[22] ISO/IEC 42006:2025 — изисквания към органите за тяхната сертификация.

[23] ANAB, публични програми за акредитация в областта на ИИ.

[24] Африкански съюз, Континентална стратегия за ИИ, 2024 г.

[25] ISO–IAF, съвместно комюнике за климатичните съображения, февруари 2024 г.

[26] Директива (ЕС) 2024/825.

[27] ICVCM, решение за осем методологии за възобновяема енергия, 06.08.2024 г.

[28] ICVCM, последващи решения по оценяване на методологии, 2026 г.

[29] PerilScope, „The TIC Council Position on the AI Omnibus“, 27.04.2026 г.
Архив на ЕИРП (ERPI Archive).

[30] ISO, IEC и ITU, Световен ден на стандартизацията 2026.