EU CyberNet

The Certificate Is Not the Control

Assurance at Scale, How It Fails and What Europe's New Conformity Regime Can Learn Before It Reaches Full Speed

- Andrew Amaro

EU CyberNet Expert Series
No 10
2026

about

Andrew Amaro



Andrew Amaro is the founder of Klavan Security, an Ottawa-based cybersecurity firm, and a former member of the Canadian Security Intelligence Service's technical operations. He writes the Shadow Tactics newsletter on intelligence, national security and cybersecurity. He has been a member of the EU CyberNet Expert Pool since January 2025.

summary

The temptation every security regime faces

Verifying that an organisation is secure is slow, expensive and depends on skilled people. Accepting a document that says it is secure is fast and cheap. When the volume of verification a system demands grows faster than the capacity to perform it, the document quietly takes the place of the thing it was meant to describe.

This paper argues that this substitution is not an occasional lapse by individual auditors or vendors. It is a predictable outcome of how assurance markets are built. It draws on three cases from outside the current EU cyber framework: an alleged large-scale failure in the North American SOC 2 attestation market in 2026, an older European precedent from the certificate authority world, and Canada's two attempts at a national cyber certification for suppliers. It then asks what these cases mean for the European Union, which is about to generate more demand for cybersecurity attestation than at any point in its history through the Cyber Resilience Act, NIS2 and the AI Act.

The aim is not to argue against certification. Done properly, certification is one of the few tools that can carry trust across long supply chains. The aim is to identify the conditions under which it stops working, so that Europe can design around them while its regime is still being built.

Anatomy of a Failure: the 2026 SOC 2 Case

SOC 2 is an attestation framework maintained by the American Institute of Certified Public Accountants (AICPA), under which an independent CPA firm examines a service organisation's controls. In North America it has become the default gate for selling software to enterprises: many buyers will not start procurement without a report.

In March 2026, an anonymous whistleblower writing as "DeepDelver" published an analysis of a leaked spreadsheet linked to Delve, a venture-backed compliance automation start-up that marketed SOC 2 and ISO27001 readiness in days rather than months. [1][2] Working from 575 leaked documents, the analysis found that a characteristic sentence from the supposedly company-specific system description appeared in 493 of 494 SOC 2 reports, that a sentence containing the same grammatical error appeared in 492, and that all 259 Type II reports carried identical test procedures and conclusions, including the same four controls declared untestable for every client. [1][2] It further alleged that draft auditor conclusions existed before clients had supplied the information an examination would require, and that clients were routed to a small network of audit and certification firms whose stated US and UK presence resolved, on the public record, to mailbox addresses or dormant registrations. [1] The same network allegedly issued ISO 27001 certificates, the standard European buyers lean on most. [1] Follow-up posts, drawing on material supplied by a company insider, alleged that staff had told a client it was acceptable to record a board meeting that never took place as audit evidence, and that a December 2024 internal planning document acknowledged uncertainty over whether the platform's controls covered all HIPAA requirements. [1] Delve denied the allegations, stating that it is an automation platform, does not conduct audits, and that final reports are issued solely by independent auditors; a later statement maintained that it has never signed or issued an audit report. [3] One of the named audit firms publicly denied any ties to Delve. [1] Delve parted ways with Y Combinator in April 2026. [4] To the author's knowledge, the allegations have not been adjudicated.

Whatever the final finding, the profession's response is telling. Through the Spring of 2026 the AICPA published guidance on the use of software tools in SOC examinations, ethics guidance on business arrangements between audit firms and tool providers, and, in May, direction to peer reviewers to examine whether high-volume SOC 2 engagements were overly standardised, overly fast or overly dependent on third-party platforms, with expanded oversight from June 2026. [5][6] An AICPA vice president observed that some firms were leaning too heavily on third-party platforms without applying the professional judgement the standards require. [5]

Three structural lessons stand out.

The payer is not the party at risk. The start-up pays for the report; its enterprise customersrely on it. For the payer, the incentive is speed and price, not rigour.

The gate checked for presence, not substance. Procurement asked "do you have a SOC 2?" rather than "what did the examination test, and who performed it?" A report can answer the first question perfectly and be worthless for the second.

The failure was detectable, but only from above. No individual buyer ever saw 494 reports side by side. The pattern became visible only to someone holding the population view, and the whistleblowers needed nothing more sophisticated than a text search across the files to reveal it. This point matters for Europe, because regulators and notifying authorities are precisely the actors who can hold that view.

Not a New Problem: Lessons Europe Has Already Paid for

Europe has met this failure mode before, twice in instructive ways.

DigiNotar was a Dutch certificate authority whose certificates were trusted by browsers and used within the Dutch government's PKIoverheid infrastructure. In 2011 attackers compromised it and issued fraudulent certificates, including for google.com, which were then used to intercept the communications of users in Iran. The forensic investigation commissioned by the Dutch government found outdated and unpatched software on public-facing servers, weak shared credentials, missing antivirus protection and ineffective separation of critical components. [7] DigiNotar operated under an audited accreditation regime. It was declared bankrupt within weeks of the breach becoming public. The lesson is that an audit describes what the auditor examined during a window; it does not describe what an attacker will find on a given day, and the gap between the two can stay invisible until it is catastrophic.

The second precedent comes from product safety. In the Poly Implant Prothèse (PIP) breast implant scandal, revealed in 2010, a manufacturer substituted unapproved industrial-grade silicone for medical-grade material while its quality system remained under notified body surveillance through announced audits. Europe's response was instructive: Commission Recommendation 2013/473/EU called for unannounced audits of manufacturers, and the MedicalDevices Regulation (EU) 2017/745 later tightened notified body oversight. [8][9] In other words, the New Legislative Frameworkhas already learned that a scheduled inspection tests what an organisation chooses to show.

Two Ways to Break a Gate: the Canadian Experience

Canada illustrates the opposite failure mode, and then a partial recovery.

CyberSecure Canada, launched in 2019, offered small and medium-sized enterprises a voluntary certification against a short baseline of thirteen sensible controls covering areas such as patching, backups, access control and multi-factor authentication. [10] The controls were reasonable. The problem was that no buyer required them. Without a procurement consequence, few SMEs had a commercial reason to pay for certification, and in the author's assessment the programme never became a market requirement.

Its successor, the Canadian Programme for Cyber Security Certification (CPCSC), was announced in Budget 2023 for defence suppliers and built on ITSP.10.171, a Canadian adaptation of NIST SP 800-171. An evaluation published by Public Services and Procurement Canada in January 2026 found that 5 of 26 deliverables had been completed on time, and that the bilateral reciprocity originally envisaged with the US Cybersecurity Maturity Model Certification (CMMC) was not possible under the current CMMC rule, leaving suppliers serving both markets with duplicated cost. [11] In April 2026 the government introduced Level 1, required in select defence contracts from Summer 2026. [12] Level 1 is an annual self-assessment against 13 controls; Level2, a third-party assessment against 98 controls, is due to enter select contracts in Spring 2027. [13]

The United States took a different path. CMMC was over-engineered in its first version, then consolidated into three levels in CMMC 2.0, but the enforcement mechanism never moved: no certification, no Department of Defence contract. [14]

Set against the SOC 2 case, the pattern is clear. Canada's first scheme had substance without a gate. The SOC 2 market had a gate without an integrity check. Both produced organisations that believed they were protected. A working assurance regime needs both: a consequence for not participating, and a mechanism that ensures participation means something.

One further observation links all of these schemes. Their entry tier, whether CPCSC Level 1, CMMC Level 1 or the default category under the EU Cyber Resilience Act, relies on self-declaration. That is a reasonable design choice for scale. It also means the integrity of the whole pyramid depends on whether anyone ever checks the base.

Why This Matters for Europe Now

The EU is building the largest cybersecurity conformity system in the world, across several instruments at once.

The Cyber Resilience Act. Regulation (EU) 2024/2847 entered into force in December 2024. Its vulnerability and incident reporting obligations apply from 11 September 2026, and full application, including conformity assessment and CE marking, follows on 11 December 2027. [15][16] Most products fall in the default category, where manufacturers may self-assess. Higher-risk categories require notified body involvement. The rules for notifying those bodies have applied since 11 June 2026, and Member States are to strive for a sufficient number of notified bodies by 11 December 2026 to avoid bottlenecks; as of mid-2026, none had yet been designated in the Commission's NANDO database. [17]

NIS2. Article 21(2)(d) of Directive (EU) 2022/2555 requires essential and important entities to address supply chain security, including the security-related aspects of their relationships with direct suppliers and service providers. [18] In practice, a very large number of entities will discharge part of that obligation by collecting supplier certificates, attestations and questionnaires, because those are the artefacts a supervisor can inspect.

The AI Act. The Digital Omnibus on AI, Regulation (EU) 2026/1744, deferred the obligations for stand-alone high-risk AI systems, including conformity assessment, to 2 December 2027, and for AI embedded in regulated products to 2 August 2028. [19] Among the reasons given were the late arrival of harmonised standards and the delayed establishment of governance and conformity assessment frameworks at national level. [20] Put these together and the conditions look familiar. Demand for attestation will rise sharply against fixed legal deadlines. The supply of qualified assessors is forming late. The entry tier relies heavily on self-declaration. And downstream buyers under NIS2 will need artefacts to show their own supervisors. These are close to the exact conditions under which the SOC 2 market produced what might be called compliance-shaped objects: documents with the form of assurance and little of its substance. Readiness platforms marketing fast CRA and NIS2 compliance already exist. Many will do honest work. The market structure, left alone, will reward the fastest.

Europe does start from a stronger position. Notified bodies are designated and monitored by national authorities, and the New Legislative Framework carries decades of experience in product safety, including the hard lessons of cases such as PIP. The question is whether those lessons are applied deliberately to cybersecurity before December 2027, rather than relearned after it.

Five Design Principles

1. Make the population view someone's job. The SOC 2 pattern was visible only across hundreds of reports. Notifying authorities and market surveillance authorities could routinely sample declarations of conformity, technical documentation and assessment reports, and apply simple similarity analysis to flag templating, implausible timelines and recurring assessor relationships. This is inexpensive and directly targets the failure mode. Authorities should also follow volume when it moves. In the SOC 2 case, once the original firms were exposed, client engagements were reportedly transferred to other signatories, in at least one case with an assurance that ongoing observation periods would not need to restart. [1] Exposing one signatory does not remove the demand; it relocates it.

2. Keep the tool and the judge separate. Platforms that collect evidence and bodies that evaluate it should be structurally independent: no referral fees, no undisclosed commercial arrangements, no shared ownership. A recording published by the whistleblower allegedly captures the platform's leadership remarking that the signing audit firm carried the liability. [1] That is the structural risk in a sentence: the party designing the conclusions is not the party accountable for them. The AICPA's 2026 ethics guidance on tool-provider arrangements offers a starting template for closing that gap. [6]

3. Check self-declarations, sometimes unannounced. Self-assessment at the entry tier is necessary for scale, but it only works if there is a credible probability of verification. Europe already accepted this logic for medical devices after PIP. [8] Risk-based spot checks of self-declared CRA conformity would carry the same deterrent value.

4. Pair attestation with adversarial testing. An assessment describes controls during a window; a test shows what an attacker finds today. Europe already has the model in TIBER-EU and the threat-led penetration testing required under DORA for the financial sector. [21] Proportionate versions for critical suppliers and important products would help close the gap DigiNotar exposed.

5. Teach buyers to read the paper. Much of the leverage sits with the procurement officer. Useful questions include: who performed the assessment and can their accreditation be verified independently (for ISO 27001, whether the certification body is accredited by a recognised national accreditation body, which can be checked through the IAF CertSearch database); what was in scope; which controls failed testing and why; and how long was the observation period. A report that could describe any company should be treated as describing none. Capacity-building programmes, including those supported through EU CyberNet, are well placed to spread this literacy, particularly in partner countries now adopting EU-style frameworks.

Conclusion

A certificate is a promise made on behalf of an organisation to people who cannot check it themselves. Its value depends entirely on the probability that the promise was actually tested. When that probability falls, the certificate keeps its appearance but loses its meaning, and the loss stays invisible until an incident reveals it.

Europe has an advantage that the cases above did not: it can see these failure modes before its own regime reaches full scale. The CRA, NIS2 and the AI Act will almost certainly create a market for compliance-shaped objects. The real question is whether the system is designed so that those objects get found.



References

[1] DeepDelver, "Delve: Fake Compliance as a Service", Substack: Part I, 19 March 2026, *https://deepdelver.substack.com/p/delve-fake-compliance-as-a-service*; Part II Day 1, 28 March 2026, https://deepdelver.substack.com/p/delve-fake-compliance-as-a-service-61d ; Part II Post 3, 18 April 2026, *https://deepdelver.substack.com/p/delve-hawaii-edition-part-ii-post*

[2] IANS Research, "Delve Allegations Expose Weak Points in Modern Compliance", 2026. https://www.iansresearch.com/resources/all-blogs/post/security-blog/2026/04/19/delve-allegations-expose-weak-points-in-modern-compliance

[3] ComplianceHub.Wiki, "The Delve Scandal: When Your SOC 2 ReportIs Just a Template", March2026 (includes Delve's formal response), https://compliancehub.wiki/delve-compliance-startup-fake-soc2-audit-scandal/ ; Delve, "Delve sets the record straight on anonymous attacks", 2026, https://delve.co/blog/delve-sets-the-record-straight-on-anonymous-attacks

[4] TechCrunch, "Embattled startup Delve has parted ways with Y Combinator", 4 April 2026. https://techcrunch.com/2026/04/04/embattled-startup-delve-has-parted-ways-with-y-combinator/

[5] Journal of Accountancy, "AICPA guides peer reviewers to address SOC 2 risks", May 2026. https://www.journalofaccountancy.com/issues/2026/may/aicpa-guides-peer-reviewers-to-address-soc-2-risks/

[6] Journal of Accountancy, "SOC Engagements: Ethics Risks With Tool Providers", April 2026. https://www.journalofaccountancy.com/issues/2026/apr/soc-engagements-ethics-risks-with-tool-providers/

[7] Fox-IT, "Black Tulip: Report of the investigation into the DigiNotarCertificate Authority breach", commissioned by the Dutch Ministry of the Interior and Kingdom Relations, 2012.

[8] Commission Recommendation 2013/473/EU on the audits and assessments performedby notified bodies in the field of medical devices. https://eur-lex.europa.eu/eli/reco/2013/473/oj

[9] Regulation (EU) 2017/745on medical devices.https://eur-lex.europa.eu/eli/reg/2017/745/oj

[10] Innovation, Science and Economic Development Canada, CyberSecure Canada. https://ised-isde.canada.ca/site/cybersecure-canada/en

[11] Public Services and Procurement Canada,"Evaluation of the Canadian Programfor Cyber SecurityCertification", January 2026. https://www.canada.ca/en/public-services-procurement/corporate/transparency/evaluation-report/2025-2026/evaluation-cyber-security-certification.html

[12] Public Services and Procurement Canada,"Government of Canada introduces Level1 of Canadian Program for Cyber Security Certification", April 2026. https://www.canada.ca/en/public-services-procurement/news/2026/04/government-of-canada-introduces-level-1-of-canadian-program-for-cyber-security-certification.html

[13] Mondaq, "Canada Just Made CPCSC Mandatory. Your Next DefenceContract Depends On It", 2026. https://www.mondaq.com/canada/government-contracts-procurement-ppp/1774586/

[14] US Department of Defense, Cybersecurity Maturity Model Certification (CMMC). https://dodcio.defense.gov/CMMC/

[15] Regulation (EU) 2024/2847(Cyber Resilience Act). https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[16] Hogan Lovells, "EU Cyber Resilience Act: Key 2026 milestones toward CRA compliance", 2026. https://www.hoganlovells.com/en/publications/eu-cyber-resilience-act-getting-ready-for-cra-compliance-in-2026

[17] CyberResilienceAct.eu, "On 11 June 2026, the CRA's Rules on Notified Bodies Started to Apply, but None Are Designated Yet", 2026. *https://www.cyberresilienceact.eu/fr/news/cra-notified-bodies-rules-apply-11-*june-2026.html

[18] Directive (EU) 2022/2555(NIS2), Article 21. *https://eur-lex.europa.eu/eli/dir/2022/2555/oj*

[19] Cooley, "Digital AI Omnibus DelaysKey Deadlines, Introduces New Rules", 2026.https://cdp.cooley.com/digital-ai-omnibus-delays-key-deadlines-introduces-new-rules/

[20] Digital Omnibus on AI, Regulation (EU) 2026/1744, recitalsand Article 1 (consolidated explorer). https://artificialintelligenceact.eu/ai-act-explorer/digital-omnibus/

[21] European Central Bank, TIBER-EU framework. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

The Certificate is Not the Control
Assurance at Scale, How It Fails and What Europe's New Conformity Regime Can Learn Before It Reaches Full Speed
Andrew Amaro

EU CybetNet Expert Series, No 10, 2026

© EU CyberNet 2026

EU CyberNet

Funded by the European Union

EU GLOBAL THREATS PROGRAMME

Views and opinions expressed are those of the author only and do not necessarily reflect those of the European Union or the EU CyberNet. Neither the European Union nor EU CyberNet can be held responsible for them.