Governing AI, Building Trust

Europe's Cybersecurity Talent Imperative in the NIS2 Era

Gustavo Frega
Senior Manager, Academic Strategy & Business Partnerships

More regulation.
More AI tools.
More breaches.

Why?

More regulation than ever. More AI tooling than ever. And yet — according to our own research — the majority of cybersecurity teams are still understaffed, and fewer than half feel confident they can respond to threats.

This is not a technology problem. It is a talent and governance problem.

160K+ entities now subject to NIS2 across the EU

55% of organisations say their cybersecurity team is understaffed

41% are confident in their team's ability to detect & respond to threats

Sources: European Commission NIS2 Implementation Report · ISACA State of Cybersecurity 2025 (n=3,812)

AI Is Rewriting the Rules

And the rulebook was already incomplete.

It's a governance crisis in the making

Attack Acceleration

AI lets threat actors automate phishing at scale, generate convincing deepfakes, and find vulnerabilities faster than any human team can respond.

Governance Blindspot

Most organisations deploy AI faster than they can govern it — creating compliance gaps invisible to existing audit and risk frameworks.

Skills Obsolescence

The cybersecurity skills of 2022 are already partly outdated. AI demands a new competency taxonomy no curriculum has fully mapped.

Regulatory Latency

NIS2 was written pre-generative-AI. Its intersection with the EU AI Act creates compliance complexity few organisations are ready for.

THE MOST AMBITIOUS RULEBOOK IN THE WORLD

Europe has written the rules — twice over

NIS2 — THE BACKBONE

- ✓ Risk management across 18 critical sectors
- ✓ Board-level accountability for incidents
- ✓ 72-hour incident reporting
- ✓ Sanctions up to €10M or 2% of turnover

EU AI ACT — THE NEW LAYER

- → Risk-based: unacceptable → high → limited → minimal
- → Prohibited uses banned since Feb 2025
- → High-risk obligations from Aug 2026
- → Fines up to €35M or 7% — higher than GDPR

But neither writes itself into reality. The AI Act's own harmonised standards slipped past deadline — the regulation is ready before the means to comply with it are. Rules do not execute themselves. People do.

REGULATION WITHOUT A MECHANISM

Europe has the rules. It is still missing the mechanism.

THE UNITED STATES

Mandates CMMC — Cybersecurity Maturity Model Certification — as a verified, audited requirement to win defence contracts. No certification, no contract. A regulation with both teeth and a mechanism.

EUROPE

Has NIS2 and the AI Act — but no common certification mechanism across its 27 member states. **National exceptions exist** — Spain's ENS mandates audited certification for sensitive public-sector systems — but there is no EU-wide equivalent.

THE BRIDGE: GOVERNANCE & MATURITY FRAMEWORKS

COBIT	CMMI	NIST AI RMF	ISO/IEC 42001
Enterprise IT governance	Capability maturity (ISACA)	AI risk management	AI management systems

Frameworks turn regulatory intent into operational reality — they are how an organisation proves, in a structured and auditable way, that it can govern AI. The standards Europe is still waiting for already exist in the profession.

THE REAL OBJECTIVE

Trust — specifically, Digital Trust

Trust has always been the currency of business. What is new is that we now have to produce it on top of systems that make decisions on their own. That is digital trust — and it is the whole point of governing AI.

Quality & Integrity

Systems that do what they claim — accurate, reliable, and resilient under pressure.

Transparency & Ethics

Decisions that can be explained, defended, and aligned with human values.

Accountability

Clear ownership of outcomes — someone is answerable when AI acts.

The concept belongs to the whole profession. *ISACA has given it a name and a structure — the Digital Trust Ecosystem Framework — but digital trust is the objective every framework, rule and credential ultimately serves.*

The Missing Variable

You cannot govern what you don't understand.

300,000

the cybersecurity professionals Europe is missing

A gap this size cannot be hired into existence. It has to be built — and proven.

Source: ENISA, 2024

Europe's most dangerous cybersecurity vulnerability is not a zero-day. It's a talent shortage.

55%

of organisations say their cybersecurity team is understaffed

31%

of applicants are considered well-qualified for open roles

27%

agree university graduates are prepared for real challenges

The workforce is ageing: 35% of cybersecurity professionals are aged 45–54 — and only 8% are aged 25–34. Europe is not building its next generation of cyber talent fast enough.

Source: ISACA State of Cybersecurity 2025 (global survey, n=3,812)

In an AI-accelerated threat landscape, certification is not a credential. It is infrastructure.

01

Language for Governance

NIS2 demands board-level accountability. CISM, CRISC and CGEIT give executives a shared language for managing cyber risk — not just tools for IT teams.

02

Trust Signal for Markets

Certified professionals signal verified competence to clients, regulators and partners. In public procurement and critical infrastructure it is increasingly mandatory.

03

Employers Are Pulling Back

Employer-paid certification fees dropped 11 points in one year (65%→54%) per ISACA's State of Cybersecurity 2025 — cut precisely when the crisis demands the opposite.

Building the Response

From knowledge to readiness — and from readiness to trust.

A degree is not readiness. A job title is not readiness either.

A DEGREE

proves you studied the subject — three or four years ago.

A JOB TITLE

proves someone decided to hire you — at one point in time.

REAL-WORLD READINESS

proves you can govern AI responsibly — right now, when the stakes are real.

The gap holding Europe back is not knowledge. It is readiness — the proven ability to act with judgment when AI governance actually matters. And only 27% of us believe new graduates have it.

Credentials answer the one question a degree cannot: are you actually ready?

MEDICINE	LAW	ENGINEERING	ACCOUNTING
Board Certification	The Bar Exam	Chartership	CPA / ACCA

Cybersecurity and AI governance are now high-stakes professions too — and the stakes are higher, because the technology outpaces every curriculum ever written.

Credentials are not bureaucracy. They are how a profession validates real-world readiness: an independent, continuously-updated standard of what "ready to govern" actually means. That is the role credentials like CISM, CRISC and CGEIT play — not as products, but as the bar we hold ourselves to.

THE PRACTITIONER'S MANDATE

Governing AI, Building Trust

GOVERNING AI

Not blocking it. Not rubber-stamping it. Making deliberate, accountable decisions about how AI is deployed, monitored and controlled — so the organisation can move fast without losing control.

BUILDING TRUST

Trust is not a feeling. It is an output — what you produce when governance is visible, competence is proven, and decisions can be defended. Trust is the deliverable.

You are the person who turns AI from a liability into a trusted capability. That is the job. That is the future of this profession.

THE DESTINATION

The Trust Economy

Europe will not win the cybersecurity challenge with regulation alone.
It will win it with people who know how to govern.

- Organisations that govern AI well will be the ones clients and partners trust.
- Nations that invest in certified talent will lead Europe's digital economy.
- Communities that bridge academia and industry will shape the next generation.

The foundation of the trust economy is built one skilled, certified professional at a time.

Governing AI is the mandate.

Building trust is the outcome.

Both depend on you.

Thank you.

Questions & Discussion

Gustavo Frega
Senior Manager, Academic Strategy & Business Partnerships
gfrega@isaca.org
https://www.linkedin.com/in/gustavofrega/

KEY TAKEAWAYS

01 NIS2 and the EU AI Act set the rules — but rules alone don't create capability.

02 Frameworks (COBIT, CMMI, NIST AI RMF, ISO 42001) turn regulation into practice.

03 Europe has the regulation; it still lacks the mechanism the US built with CMMC.

04 Readiness, not a degree, is the real deliverable — and credentials prove it.

05 The mandate is ours: govern AI, and earn digital trust


ISACA®