CAGI

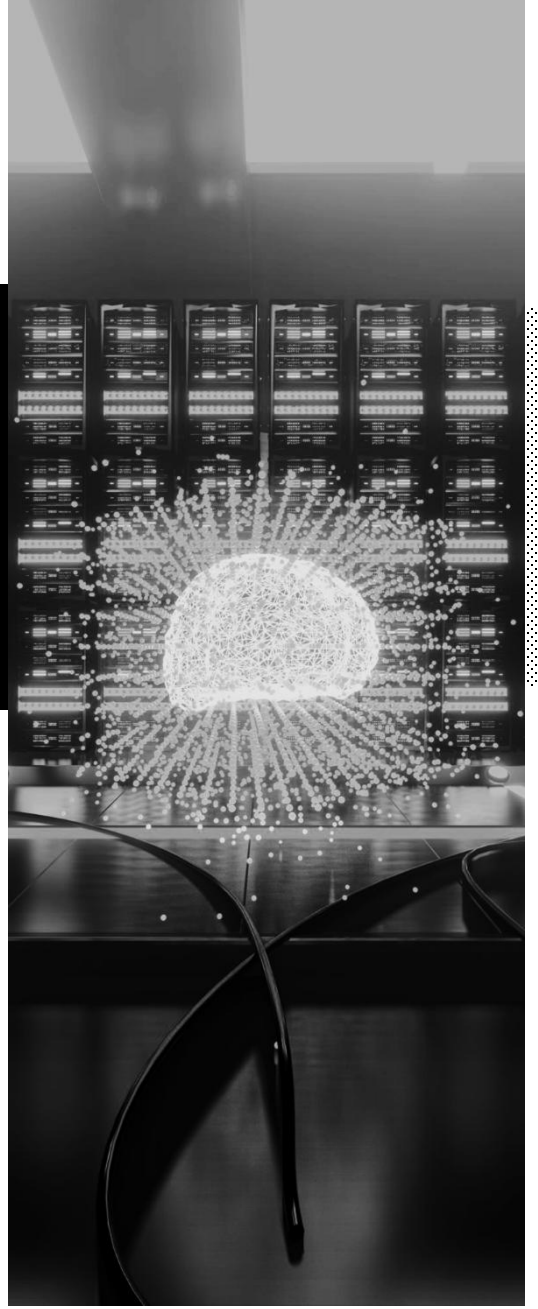
The Cybersecurity & AI Governance Initiative

Introducing CAGI

Shaping Trust in the Digital Future – Through Collaboration

Welcome to CAGI

The Cybersecurity & AI Governance Initiative (CAGI) has been established as an international institute dedicated to shaping the future of **cybersecurity, AI governance, and quantum readiness**.



Our Purpose

CAGI exists to close the gap between emerging technologies and effective governance.

By uniting policymakers, industry leaders, academics, and practitioners worldwide, it will serve as the trusted global forum for developing standards, testing innovation, and building resilience.

Our Mission is to establish CAGI as the leading international institute dedicated to shaping the future of cybersecurity, AI governance, and quantum readiness. CAGI delivers practical frameworks, pilot projects, research, and policy engagement that empower organisations and governments to adapt, innovate, and lead in a rapidly evolving digital landscape.

What Problems are we Addressing?

AI, quantum, and emerging tech are being embedded into critical infrastructure without governance or control.

Current cybersecurity frameworks are not designed for AI-driven cyberattacks or post-quantum threats.

Businesses and governments face escalating exposure with no global body to unify standards.

“Where others analyse today’s risks, CAGI builds the frameworks for tomorrow’s”.

The Gap in Current Frameworks

Most cybersecurity frameworks (NIST CSF, ISO 27001, CIS Controls) were designed to address threats in a pre-AI, pre-quantum world. They are strong at managing traditional risks like malware, insider threats, and compliance requirements, but they are not structured to anticipate:

AI-Driven Threats: Attackers are now leveraging generative AI, adversarial algorithms, and autonomous malware. These threats evolve in real time, outpacing static frameworks that rely on periodic audits and manual controls. Traditional controls cannot account for deepfakes, AI-powered phishing, or self-adapting ransomware.

Quantum Risks: Cryptographic standards that underpin the world's digital economy (RSA, ECC) are at risk of collapse once scalable quantum computers emerge. Existing frameworks do not provide guidance on quantum-safe migration, leaving governments, financial systems, and healthcare infrastructures exposed.

Critical Infrastructure Integration: AI and quantum are already being embedded in energy grids, defence systems, transport, and healthcare. A breach here is not just a data loss event - it could cause systemic physical disruption. Current frameworks were never built to govern these new realities.

Why This Matters

Without forward-looking governance frameworks, the world risks a **structural security gap:** regulations and standards that look backwards rather than anticipating the next wave of threats.

This gap is precisely where CAGI positions itself - to provide foresight, governance, and practical frameworks that help governments, industries, and academia prepare for the technologies shaping the next decade.

Bridging the Gap

Without future-ready governance frameworks, organisations and governments are forced to rely on standards that are outdated before they are even finalised. The traditional cycle of drafting, reviewing, and publishing guidance can take years, while disruptive technologies like AI and quantum evolve in months. This creates a widening lag between innovation and regulation, where:

Attackers exploit first-mover advantage: Malicious actors adopt AI and quantum tools far faster than regulators or compliance bodies can respond.

Global inconsistency emerges: Nations and industries develop fragmented responses, leading to a patchwork of incompatible rules that increase costs and complexity for businesses.

Critical systems remain exposed: Financial institutions, healthcare networks, and national infrastructure operate under assumptions of cryptographic security and manual oversight that no longer hold.

Trust erodes: Investors, consumers, and governments lose confidence in digital systems that appear powerful but unregulated, slowing adoption of technologies that could deliver significant societal value.

The result is a global structural security gap where innovation races ahead unchecked, and oversight is perpetually behind. Closing this gap requires a new model: one that is anticipatory, agile, and internationally coordinated.

Where CAGI Fits

CAGI closes this gap by:

- Developing AI and quantum-inclusive maturity models.
- Running pilot programmes (e.g., testing quantum-safe encryption in live settings).
- Publishing foresight reports that anticipate rather than react to emerging threats.
- Providing a neutral global platform that unites governments, academia, and industry to address risks proactively.

From Foresight to Authority

How CAGI frameworks gain legitimacy and impact

CAGI does not compete with regulators or standards bodies. It operates upstream of them.

CAGI frameworks gain authority by:

- Being developed collaboratively with government, academia, and industry.
- Being tested through real-world pilots rather than theoretical alignment.
- Providing evidence of effectiveness, not declarations of compliance.
- Aligning with international standards while addressing gaps they cannot yet cover.

CAGI outputs are designed to inform regulation, guide adoption, and shape executive and board-level decision-making before risk becomes systemic.

CAGI differs from think tanks, industry groups, and compliance bodies in four critical ways:

CAGI is:

- Anticipatory, focused on plausible futures rather than past failures.
- Integrated, treating AI, cybersecurity, and resilience as a single risk domain.
- Continuous, operating alongside evolving systems rather than static audit cycles.
- Decision-focused, centred on authority, accountability, and escalation.

“CAGI exists to close the structural gap between responsibility and control created by AI-driven systems.”

Our Three Pillars Of Focus

CAGI's three pillars focus on securing the present, governing the near future, and preparing for long-term disruption.

Cybersecurity Futures helps anticipate next-generation threats, AI Governance delivers practical frameworks for responsible adoption, and Quantum Readiness equips members for the cryptographic and infrastructure shifts of tomorrow.

Together, they ensure CAGI addresses today's risks while guiding members through the transformations ahead.

Cybersecurity Futures

Anticipating global threats, infrastructure disruption, and digital risks.

Artificial Intelligence Governance

Delivering frameworks, sandboxes, and training on responsible AI.

Quantum & Future Tech Readiness

Preparing governments and organisations for post-quantum disruption.

Structure / Roles & Responsibilities

Headquarters

Role: Strategic control, standards ownership, and institutional accountability

- Holds final authority over all global frameworks, standards, and policy positions.
- Owns governance design, maturity models, accreditation, and global programmes.
- Sets mandatory operating standards for all Chapters and Working Groups.
- Exercises audit, enforcement, and sanction authority over Chapters.
- Arbitrates conflicts between Chapters, partners, and stakeholders.
- Represents CAGI in international policy and regulatory forums (UN, OECD, WEF).
- Accountable for institutional credibility, neutrality, and global consistency.

Regional & National Chapters

Role: Implementation, engagement, and evidence generation

- Operate under binding CAGI International Chapter Bylaws.
- Deliver HQ-approved frameworks, pilots, and programmes in local contexts.
- Prohibited from issuing independent standards or policy positions.
- Required to meet minimum activity, reporting, and quality thresholds.
- Subject to regular performance reviews and governance audits by HQ.
- Retain operational autonomy within defined global guardrails.

Steering Committee

Role: Independent challenge, foresight, and institutional risk oversight

- Non-executive body comprising senior industry, government, and academic leaders.
- Provides structured challenge to HQ strategy, priorities, and governance posture.
- Reviews global risk themes, emerging technology trajectories, and foresight outputs.
- Validates long-term relevance and neutrality of CAGI's work.
- Has formal escalation rights on material governance, credibility, or integrity risks.
- Does not execute operations or manage Chapters.

Member Outcomes

CAGI membership is designed to strengthen decision-making, governance capability, and institutional credibility in environments shaped by AI, cybersecurity, and emerging technologies.

Reduced Uncertainty Through Early Visibility: Members gain early insight into emerging governance, cybersecurity, and AI risk trajectories identified through CAGI's foresight work, global chapter activity, and applied pilots. This visibility enables organisations to anticipate regulatory, operational, and systemic risk before it materialises as incidents, compliance pressure, or strategic disruption.

Defensible Governance Capability: Members access practical governance frameworks and maturity models that can be applied, tested, and defended in real environments. These outputs are designed to support executive and board-level accountability, providing structures that withstand regulatory, audit, and public scrutiny rather than aspirational policy statements.

Evidence, Not Theory: Through participation in pilots, testbeds, and applied research, members engage with governance models that are exercised in live conditions. This provides evidence of what works, what fails, and where controls degrade, enabling informed adoption rather than theoretical alignment.

Meaningful Influence Without Capture: Members contribute expertise, challenge assumptions, and inform the evolution of future governance models while preserving CAGI's independence and neutrality. Influence is exercised through participation and evidence generation, not through control of outcomes or policy positions.

Institutional Credibility and Standing: Membership signals serious engagement with accountable AI and cybersecurity governance. Participation in a neutral, evidence-led institute strengthens organisational credibility with regulators, partners, investors, and stakeholders without conflating governance with product promotion or compliance marketing.

"CAGI membership is explicitly outcome-driven."

Member Benefits

CAGI membership is not passive access. It is active participation in governing the technologies shaping trust, risk, and decision-making. Members gain access to:

Immediate Benefits (Available at Join)	
Secure Member Portal	Central access to all research, frameworks, and working group outputs.
Global Research Library	Exclusive governance frameworks, maturity models, and benchmarking reports.
Accredited Learning and Certification	Structured training programmes in AI governance, cybersecurity governance, and future technology readiness.
Mentorship Programme	Guided engagement with senior leaders from government, industry, and academia.
Global Events and Summits	Priority invitations and member pricing for CAGI's flagship international events.
Member Directory and Global Visibility	Verified listing in a global index connecting professionals across multiple regions and sectors.
Local Chapter Engagement	Participation in national and regional chapters aligned to a consistent global governance model.
Awards and Recognition	Annual recognition for leadership, innovation, and contribution to governance.
Policy Engagement	Structured opportunities to inform international discussions and consultations with global institutions.

Extended Benefits (As CAGI Expands)

CAGI membership is designed to deliver immediate value while enabling members to shape future governance models for AI, cybersecurity, and emerging technologies.

As CAGI scales, members gain access to:	
Early Access to Research and Briefings	Advance release of CAGI whitepapers, foresight reports, and policy briefings prior to public publication.
Governance Insider Updates	Regular intelligence bulletins covering AI regulation, cybersecurity futures, and emerging global standards.
Priority Access to Events	Early registration for webinars, executive briefings, and international chapter launch events.
Professional Credentialing	Use of verified CAGI membership and Founding Member credentials across professional profiles and communications.
Early Working Group Participation	Direct contribution to the first governance frameworks, pilots, and maturity models developed by CAGI.
Thought Leadership Opportunities	Ability to publish insights and commentary through the CAGI platform and global professional networks.
Early Eligibility for Leadership Roles	Priority consideration for chapter leadership, advisory roles, and working group appointments as regions launch.

SMB/Start-up Membership - $4,000

SMB and Start-Up Membership enables organisations to embed governance early, providing the insight, credibility, and access needed to manage risk and make informed decisions as they grow.

Benefits

Targeted Insight
Access to governance insight that would otherwise require significant internal investment, enabling smaller organisations to understand evolving AI and cybersecurity risk and expectation.

Credibility and Positioning
Association with a governance-led initiative, strengthening trust with customers, partners, and investors who are increasingly assessing accountability, not just capability.

Practical Guidance
Structured guidance on approaching AI and cybersecurity governance without enterprise-level overhead, allowing early-stage teams to make informed, defensible decisions.

Community Access
Connection to a global community across industry, government, and academia, providing exposure to real challenges, perspectives, and collaboration opportunities.

Commercial Visibility
Visibility within a curated ecosystem aligned to governance-led innovation, supporting partnership development and market entry.

Scalable Foundation
A clear starting point for building governance maturity early, avoiding costly correction as the organisation grows.

5 Included Membership Slots
Five individual memberships, enabling key team members to engage directly, build internal capability, and align early-stage decisions around governance.

SMB / Start-Up Membership embeds governance early, before scale makes failure expensive

Corporate Membership - $20,000

Corporate Membership positions organisations at the centre of AI and cybersecurity governance, providing the influence, insight, and access required to maintain control, demonstrate accountability, and operate with credibility in an increasingly scrutinised environment. Benefits Include:

Strategic Influence
Direct involvement in shaping governance models, contributing to working groups and cross-border initiatives, with a pathway to advisory and steering roles based on expertise.

Intelligence Advantage
Early access to governance frameworks, regulatory direction, and strategic insight translated into clear business and board-level impact.

Executive Access
Invitation-only engagement with senior leaders, regulators, and peers through focused roundtables and closed discussions on accountability and decision-making.

Organisational Capability - 25 Transferable Memberships
Twenty-five transferable memberships enabling cross-functional engagement and alignment across technical teams and leadership, embedding governance throughout the organisation.

Commercial Positioning
Positioning as a governance-aligned organisation with enhanced credibility, early visibility into procurement expectations, and access to a curated ecosystem of partners.

Operational Enablement
Access to maturity models, practical guidance, and scenario-based exercises to strengthen governance capability and align accountability with decision authority.

Visibility with Substance
Speaking and feature opportunities tied to meaningful contribution, reinforcing credibility through association with governance-led outputs.

Government Engagement
Structured access to government and regulatory stakeholders, supporting alignment with national priorities and participation in public-private initiatives.

Corporate Responsibility in the AI Era

Corporate Social Responsibility (CSR) and Corporate Digital Responsibility (CDR) are no longer peripheral considerations. As AI systems move from support functions into active decision-making roles, organisations are expected to demonstrate clear accountability for how technology influences outcomes, risk, and society.

CAGI provides a structured and credible mechanism to support this responsibility at both an operational and strategic level.

Through participation, organisations move beyond statements of intent and into demonstrable action. This includes contributing to the development of governance frameworks, engaging in cross-sector dialogue, and aligning internal practices with emerging expectations around transparency, accountability, and ethical use of AI.

This directly supports Corporate Digital Responsibility by ensuring that AI and cybersecurity systems are not only effective, but governed in a way that is defensible, auditable, and aligned with societal expectations. It also strengthens broader CSR positioning by evidencing active contribution to industry-wide solutions, rather than isolated internal compliance efforts.

In an environment where trust is increasingly determined by how technology is governed, not just how it performs, participation in CAGI enables organisations to show leadership in responsible innovation. It demonstrates that governance is embedded by design, not applied retrospectively.

This aligns with the growing expectation that organisations must evidence control over AI-driven decisions, not simply deploy them, reinforcing that governance is the foundation of trust and long-term credibility.

Sponsorship Programme

The CAGI Sponsorship Programme is designed for organisations that recognise cybersecurity, artificial intelligence, and digital governance as material to long-term resilience, trust, and market access.

Sponsorship provides structured participation in the development of applied governance frameworks, pilots, and maturity models, offering early visibility into emerging direction and the opportunity to contribute operational insight before expectations are finalised. It is not a branding or promotional programme, but a governance engagement model grounded in credibility, neutrality, and practical outcomes.

With clearly defined sponsorship tiers, organisations can engage at an appropriate level of maturity and influence, from enterprises seeking strategic leadership and advisory roles, to growing organisations and early-stage innovators building governance awareness and credibility as they scale.

Sponsorship enables organisations to collaborate with peers, policymakers, regulators, and academia in shaping responsible practice, reducing long-term risk, and strengthening trust across the digital ecosystem.

Sponsorship Programme - Tiers

$25,000 pa

- 40 transferable CAGI memberships
- Direct participation and leadership roles
- Full early visibility
- Closed executive forums and regulator-facing engagement

$10,000 pa

- 10 transferable CAGI memberships
- Invitation-only eligibility for Steering Committee
- Active participation in relevant working groups
- Early visibility Credibility signalling with enterprise buyers, partners, and stakeholders

$2,500 pa

- 5 transferable CAGI memberships
- Participation in appropriate working groups and forums
- Access to governance briefings, insight sessions, and applied learning
- Recognition as an Associate Sponsor

$1,200 pa

- 2 CAGI memberships
- 12-month fixed entry programme designed for very early-stage startups
- Access to governance briefings and selected forums,
- Recognition as an Innovator
- Progression pathway

Academia & Research

Academic and research partnerships provide the rigour, innovation, and credibility that make CAGI the trusted authority in cybersecurity, AI governance, and quantum readiness."

Key Points:

- **Joint Research:** Partner with universities and labs to co-develop studies, whitepapers, and foresight reports in cybersecurity, AI, and quantum.
- **Curriculum Collaboration:** Work with academic partners to integrate CAGI frameworks into degree programmes and professional training.
- **Shared Datasets:** Enable access to anonymised data and benchmarking results, supporting research on governance and risk.
- **Innovation Testbeds:** Engage students and researchers in pilot projects to test real-world applications of quantum-safe cryptography, AI governance models, and cyber resilience.
- **Talent Pipeline:** Create opportunities for top academic talent to engage with industry and government through internships, fellowships, and research grants.
- **Global Credibility:** Partnerships with world-leading universities and institutes strengthen CAGI's authority in international policy debates.

Contact Us

www.thecagi.com

CAGI

Shaping Trust in the Digital Future