

MAGAZINE

OCTOBER 2026
ISSUED QUARTERLY
VOLUME 11

GRC EGYPT

ANCIENT SYMBOLS. MODERN PRINCIPLES.

The symbols are presented not as decoration, but as visual frameworks for understanding how organizations remain responsible, protected, adaptable, and resilient.

EVOLVE

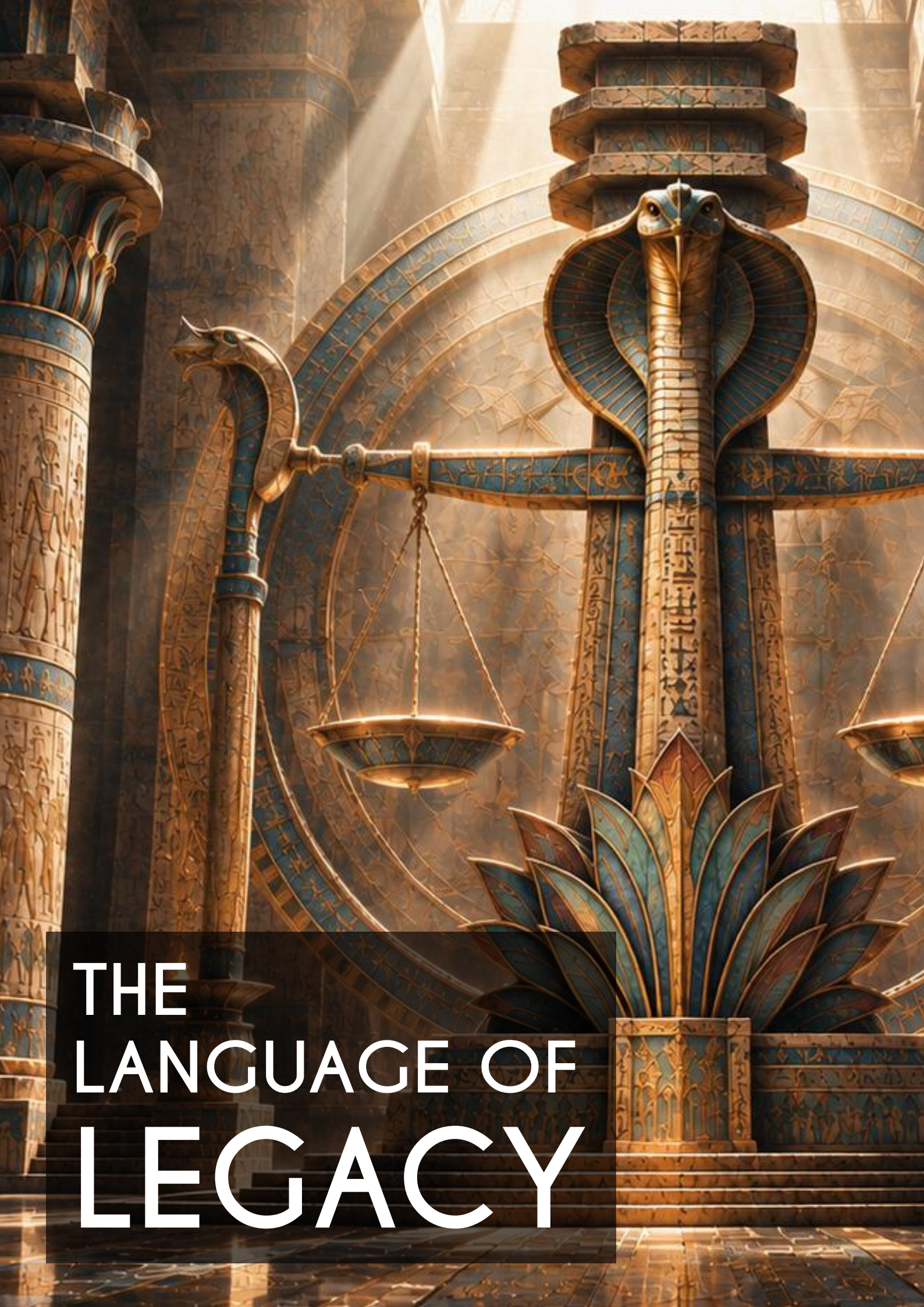
EVOLVE reflects how timeless Egyptian principles of continuity, protection, stability, balance, transformation, and control evolve into modern GRC practices—helping organizations adapt, strengthen, and build for the future.

THE LANGUAGE OF LEGACY

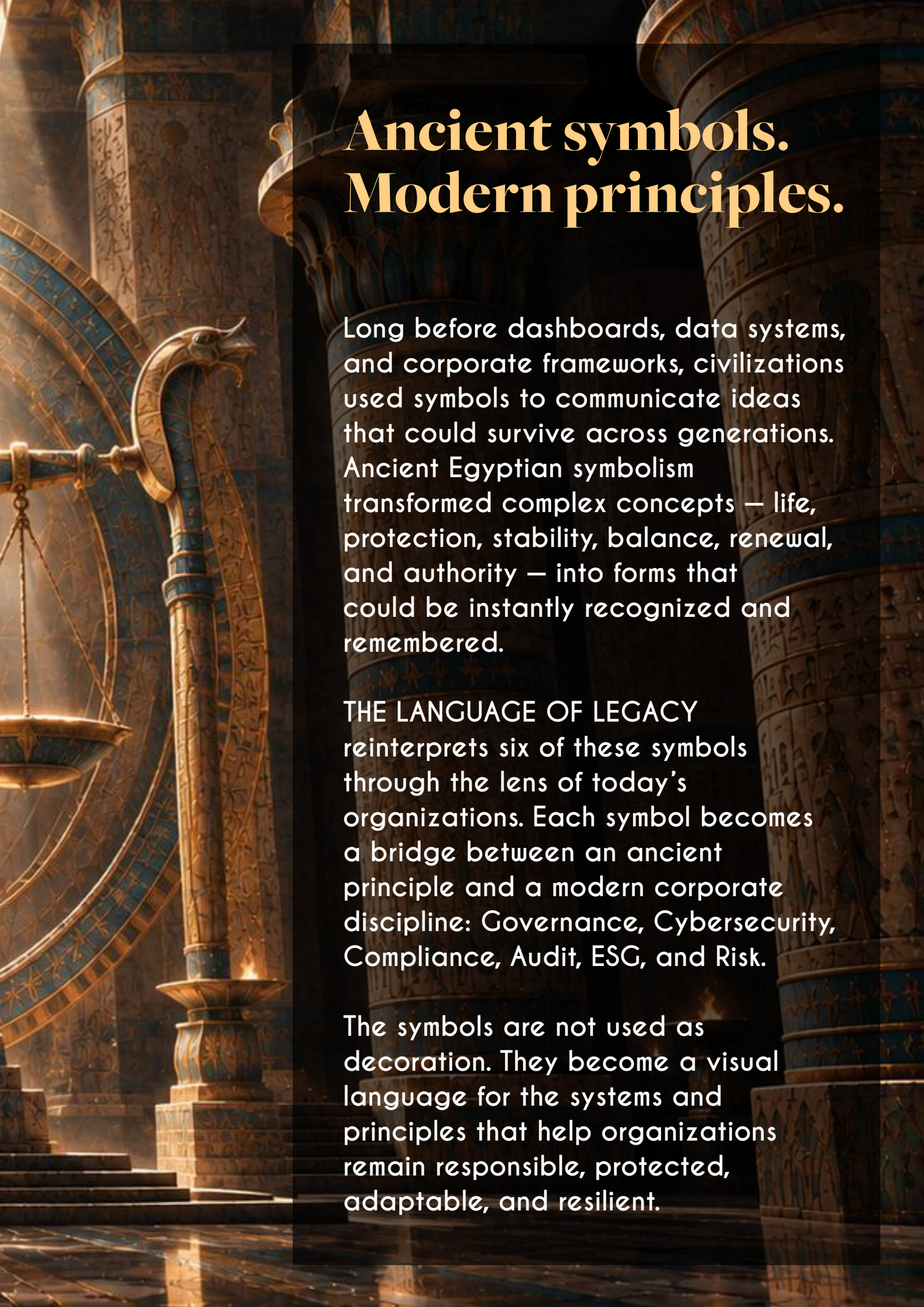
GRC Summit Egypt is a yearly edition of a tradition, bringing together leaders, experts, and academics to explore innovative approaches to digital governance. The summit will focus on empowering leaders with the knowledge and tools to build resilient and effective digital governance that can meet the challenges of the future. Also, provide a platform to explore the latest technological advancements and their impact on governance structures in the MENA region.



GRC Summit Egypt 2026



THE LANGUAGE OF LEGACY

The background image is a detailed, atmospheric rendering of an ancient Egyptian temple interior. On the left, a large, ornate scale of justice (Was scales) is visible, featuring a serpent-headed Was symbol. The temple is filled with massive columns covered in hieroglyphs, and the lighting is dramatic, with beams of light filtering through the architecture. The overall tone is historical and majestic.

Ancient symbols. Modern principles.

Long before dashboards, data systems, and corporate frameworks, civilizations used symbols to communicate ideas that could survive across generations. Ancient Egyptian symbolism transformed complex concepts — life, protection, stability, balance, renewal, and authority — into forms that could be instantly recognized and remembered.

THE LANGUAGE OF LEGACY reinterprets six of these symbols through the lens of today's organizations. Each symbol becomes a bridge between an ancient principle and a modern corporate discipline: Governance, Cybersecurity, Compliance, Audit, ESG, and Risk.

The symbols are not used as decoration. They become a visual language for the systems and principles that help organizations remain responsible, protected, adaptable, and resilient.

Alaa El Zohairy's Words

Filling the Protection Gap - Insurance role in Africa to mitigate the climate risks

Global disaster losses have exceeded \$200 billion annually over the past decade, with uninsured losses accounting for more than half of the total. This highlights the need for new financing structures to mobilize private capital alongside governments and insurers.

Insurance should be considered part of the investment architecture, not simply a protection product purchased after an investment is made. It can transfer physical and operational climate risk away from investors and project operators, protecting assets and cash flows, improving project bankability and potentially reducing financing costs. The recommended sequence is: climate-risk assessment — resilience investment — insurance/risk transfer — improved project risk profile — greater investor confidence — increased access to finance.

In Africa, where 87% of tracked climate finance comes from international sources, while the continent has approximately USD 2.4 trillion in domestic institutional assets. Insurance companies can contribute not only as underwriters, but also as investors in green bonds and climate-resilient infrastructure. The opportunity is to use insurance, Takaful, reinsurance and blended finance together to make climate-resilient projects more



President of the Insurers Federation of Egypt
And Managing Director of GIG Egypt

bankable and investable.

The protection gap remains significant. Across Africa, 97% of farmers were still without agricultural insurance in 2023, while agricultural insurance represented only 1.6% of total African non-life premiums. African agricultural insurance premiums were approximately USD 322 million in 2020, less than 1% of the global agricultural insurance market. The gap is particularly important in agriculture, climate-resilient infrastructure, catastrophe risk financing, renewable energy

and protection for SMEs exposed to climate risks. SMEs supporting Africa's agri-food system alone face an annual financing gap of more than USD 100 billion.

The opportunity is not limited to traditional crop insurance. Parametric and index-based insurance, satellite data, digital distribution and technology-enabled solutions can make climate protection faster, more affordable and more scalable. Insurance can consequently play three interconnected roles: protecting farmers and businesses from climate shocks, enabling investment by reducing financial uncertainty, and mobilizing capital by making climate-related projects more investable.

Egypt provides a clear illustration. The Insurance Federation of Egypt is working with reinsurers and reinsurance brokers on climate-risk solutions, including consideration of a National Catastrophe Pool.

No single institution can close the climate-insurance and financing gap alone. The strongest models combine governments, insurers, reinsurers, banks, investors, development institutions and technology providers. Insurance should be integrated into the project from the beginning: assess climate risk, invest in resilience, allocate risks clearly, and use

insurance, reinsurance or other risk-transfer mechanisms to address residual risk.

Kenya's Agriculture Insurance Programme combined insurers, government, the World Bank, reinsurers and agricultural aggregators and reached approximately 753,000 farmers across 33 counties by 2020. Kenya's Takaful experience demonstrates that climate protection can also reach vulnerable pastoralist communities.

Zambia provides another model, where insurers, banks, MFIs, government agricultural officers and other stakeholders worked together on product development, training, distribution and reinsurance, with approximately 160,000 farmers benefiting during the 2022/23 season. Senegal's AIRCM programme shows that insurance must work alongside adaptation: prevention and resilience measures should reduce the underlying risk, while insurance and reinsurance address the residual risk.

What I take from these African experiences is that the challenge is not simply to develop more insurance products. We need to build the ecosystem around them. Kenya shows the value of index insurance and reinsurance; Zambia shows the importance of capacity building and integrating insurance with agricultural finance; Senegal shows that insurance must work alongside adaptation; and Takaful shows that climate protection can reach vulnerable communities. The common denominator is partnership.

I believe the first step is to change the position of insurance in the investment process. Insurance should not come after the investment decision. Climate risk should be assessed at project inception, resilience measures incorporated into project design, and insurance and risk transfer made part of the financing structure from the beginning.

For Africa, this is important because the continent requires approximately USD 250 billion annually in climate finance, while climate-finance flows were only around USD 30 billion in 2020. We need to use the full range of risk-transfer mechanisms: traditional catastrophe insurance, parametric insurance, risk pooling, reinsurance and, where appropriate, catastrophe bonds.

Insurance should no longer be viewed as the final layer of protection after an investment is made. It should be part of the investment architecture itself—helping measure, price and transfer climate risk, protect cash flows and assets, improve bankability and unlock capital for Africa's climate-resilient future.

CLIMATE RESILIENCE
THROUGH PARTNERSHIP



Ahmed AbdelHafez's Words

From Compliance to Cyber Resilience: Rethinking GRC in the Age of AI

For many years, Governance, Risk and Compliance (GRC) has been approached primarily as a framework for meeting regulatory requirements, documenting controls, conducting audits and demonstrating compliance. While these activities remain essential, the rapid transformation of the digital landscape is forcing organizations to reconsider what GRC should ultimately achieve.

Today, compliance is no longer the destination. Resilience is. Organizations are operating in an environment where cloud adoption, artificial intelligence, digital payments, connected devices, APIs, remote work and increasingly complex supply chains have expanded the digital attack surface dramatically. At the same time, cyber threats are becoming faster, more automated and more difficult to detect.

Artificial intelligence is accelerating this transformation on both sides. Organizations are using AI to improve detection, automate security operations, analyze risks and support decision-making. At the same time, adversaries can use AI to enhance phishing, social engineering, vulnerability discovery, malware development and other attack activities.

This creates a fundamental question for boards and executive management:

Are our GRC programs designed to demonstrate compliance, or are they actually preparing the organization to withstand disruption?

From a checklist mentality to risk-based governance

A mature GRC program should not be measured simply by the number of policies completed or audit findings closed. It should help management understand the risks that could materially affect the organization's objectives, reputation, operations and stakeholders.

This requires moving from a checklist-driven approach toward risk-based and business-oriented governance.

Cybersecurity should therefore be discussed at the board and executive level not only in terms of technologies, vulnerabilities and security controls, but also in terms of business continuity, financial exposure, regulatory obligations, customer trust and operational resilience.

The objective is not to eliminate every cyber risk. That is neither realistic nor economically sustainable. The objective is to understand the organization's most important risks, establish appropriate controls, continuously monitor the changing threat environment and ensure that the organization can respond and recover when controls fail.

AI is changing the GRC equation AI introduces a new dimension to this challenge.

Traditional risk assessments often depend on periodic reviews. However, the risk environment can now change much faster than the traditional GRC cycle.

Organizations need to consider questions such as:

- What data is being provided to AI systems?
- Where is that data stored and processed?
- Who can access AI-generated information?
- How are AI decisions validated?
- What happens when an AI model produces an incorrect or manipulated output?
- Are third-party AI services introducing new privacy, security or regulatory risks?
- Can employees use generative AI tools without adequate governance?
- How should organizations manage AI-related risks across the supply chain?

These are not purely technical questions. They are governance and risk questions.

Consequently, organizations need an AI governance model that brings together cybersecurity,



CEO Advisor for
Cybersecurity, NTRA

privacy, legal, compliance, risk management, technology and business leadership.

Digital sovereignty and data governance

For organizations operating in Egypt and the wider region, another increasingly important consideration is the governance of strategic data.

As organizations depend more heavily on international cloud platforms, SaaS applications and AI services, executives need greater visibility into where critical information resides, how it is processed, which jurisdictions may have access to it, and how the organization can maintain continuity if a service becomes unavailable.

Data governance therefore becomes an essential component of cyber resilience.

The question is no longer just: "Is our data protected?"

It should also be:

"Do we know where our critical data is, who controls the infrastructure processing it, what regulations apply to it, and whether we can continue operating if that infrastructure becomes unavailable?"

This perspective is particularly relevant for sectors such as banking, telecommunications, energy, healthcare, government and critical infrastructure, where cyber incidents can have consequences far beyond the affected IT system.

Building a resilient GRC ecosystem

The future of GRC will require closer integration between traditionally separate functions.

Cybersecurity teams cannot operate independently from risk and compliance teams. Privacy cannot be treated as a purely legal responsibility. Business continuity cannot be separated from cyber risk. And technology decisions involving cloud and AI cannot be made without considering governance and regulatory implications.

A resilient organization should establish an integrated model built around five principles:

1. Board-level accountability

Cybersecurity and technology risks should be connected directly to business objectives and discussed at the appropriate executive level.

2. Continuous risk visibility

Risk assessments should evolve from periodic exercises toward continuous monitoring of assets, threats, vulnerabilities, third parties and regulatory requirements.

3. Security and privacy by design

New digital services, AI initiatives and technology projects should incorporate security, privacy and compliance requirements from the beginning rather than as an afterthought.

4. Resilience rather than prevention alone

Organizations should assume that some controls will eventually fail and invest equally in detection, response, recovery and crisis management.

5. Intelligent use of AI

AI should become an enabler of GRC—not simply another technology risk. Organizations can use AI to analyze large volumes of risk information, identify patterns, prioritize issues and support security and compliance operations, while maintaining appropriate human oversight.

The next chapter of GRC

The GRC function is entering a new era.

The organizations that succeed will not necessarily be those with the largest number of policies or the highest number of compliance certificates. They will be those capable of translating governance and regulatory requirements into measurable business resilience.

For Egypt and the broader Middle East, this represents an important opportunity. The acceleration of digital transformation creates significant economic and societal benefits, but these benefits depend on trust.

Trust requires secure technology. Secure technology requires effective governance. Effective governance requires informed risk management. And sustainable risk management requires an organizational culture in which cybersecurity, privacy, compliance and resilience are considered business priorities rather than isolated technical or regulatory functions.

Ultimately, the goal of modern GRC should be simple: Not merely to prove that an organization complies with the rules, but to ensure that it remains trusted, secure and resilient when the rules—and the threat landscape—continue to evolve.

THE ANKH | CONTINUITY GOVERNANCE

ANCIENT SYMBOL — THE ANKH

The Ankh is one of the most recognizable symbols of Ancient Egypt and is associated with life and continued existence. Its distinctive loop and continuous form make it a natural visual expression of something that does not simply begin and end, but continues through time.

THE MODERN CONNECTION — GOVERNANCE

In a modern organization, continuity depends on governance. Leadership, accountability, decision-making structures, policies, and organizational responsibilities create the framework that allows an institution to operate today while preparing for tomorrow.

The Ankh therefore becomes a metaphor for the organizational framework that keeps an institution moving forward. Its continuous form represents the connection between leadership, accountability, responsibility, and long-term direction.

THE PRINCIPLE

“GOVERNANCE CREATES THE FRAMEWORK FOR CONTINUITY.”

True continuity is not simply about surviving change. It is about building structures strong enough to support change while preserving the principles that define the organization.



Dr. Welland Chu's Words

Coping with Unpredictable Risks in the AI Era: Unpredictable Does Not Mean Unpreparable



Artificial intelligence is moving from decision support to action. AI-enabled systems can retrieve information, invoke tools, initiate workflows, communicate with stakeholders, and influence operational outcomes. This shift—from AI that recommends to AI that acts—changes the governance question.

The key challenge is not to make every AI output perfectly predictable. It is to bound an AI system's authority, observe its actions, interrupt unsafe activity, and restore critical services when controls fail.

An unexpected model response must not automatically produce unrestricted access, irreversible authority, or an unmonitored route into critical systems. Unpredictability in reasoning need not mean unpredictability in permissions, execution paths, data access, escalation thresholds, or recovery capability.

For financial institutions, critical-infrastructure operators, and other high-consequence enterprises, the objective is not to eliminate uncertainty, but to fortify digital defence that remain effective when uncertainty materialises.

The governance challenge

Unlike traditional IT, agentic AI may interpret natural-language instructions, select tools, interact with multiple systems, consume untrusted content, and adapt its actions during execution. This creates a compounded risk profile:

- Instructions, policies, exceptions, or delegation boundaries may be misinterpreted.
- Prompt injection, poisoned data, or malicious content may influence decisions or tool use.
- Compromised identities, tokens, APIs, plug-ins, or suppliers may create excessive access.
- Automation can turn a minor error into a high-speed, high-scale event.
- Human oversight can become ineffective when workflows outpace review or lack context.

The distinctive risk is the combination of probabilistic reasoning, delegated authority, connected tools, external inputs, and machine-speed execution.

The crucial distinction is simple: an AI system may generate an unexpected output, but whether that output can trigger an unsafe or irreversible consequence is a design and governance decision.

The AI Risk Knowledge Quadrant

The Risk Knowledge Quadrant distinguishes risks that can be directly managed from those that demand learning, containment, and resilience.

- Known knowns: Meaning Understood and documented risks, Governance response Apply controls, validation, monitoring, and assurance
- Known unknowns: Meaning Recognised but unquantified risks, Governance response Use staged deployment, red-teaming, testing, and change control
- Unknown unknowns: Meaning Emergent behaviours and novel failure chains, Governance response Limit authority, contain blast radius, preserve intervention, and rehearse recovery
- Unknown knowns: Meaning Critical operational knowledge absent from AI design, Governance response Bring together business, risk, legal, security, resilience, and domain expertise



Known risks remain important. However, high-consequence AI governance depends particularly on “unknown unknowns” and “unknown knows”. Prediction alone cannot manage emergent failure; organisations must design for containment and recovery. They must also ensure that knowledge of operational dependencies, customer harm, and regulatory duties reaches AI design and deployment teams.

The essential question is: Which

AI risks can we not yet evidence, and what critical operational knowledge have we not incorporated into our control decisions?

Control architecture

The 18 controls below are not a universal checklist. They form a proportionate architecture that should strengthen as an agent’s authority, data sensitivity, external connectivity, and potential impact increase.

a. Constrain authority

1. Inventory and classify systems, data, identities, tools, and dependencies. 2. Segment and isolate. 3. Apply identity-centric zero trust. 4. Govern delegation. 5. Sandbox execution and control egress.

b. Protect the environment

6. Harden APIs and interfaces. 7. Protect the supply chain. 8. Separate secrets from execution. 9. Monitor runtime activity.

c. Observe and intervene

10. Enforce policy as code. 11. Analyse anomalous behaviour. 12. Integrate risk intelligence. 13. Automate authorised containment. 14. Adopt active defence. 15. Maintain immutable audit trails.

d. Recover with confidence

16. Apply meaningful human oversight. 17. Rehearse AI-specific incident response. 18. Integrate AI failure into crisis management and trusted-baseline recovery.

The governing principle is clear: do not rely on a model to police its own authority. Access, monitoring, revocation, and escalation must remain independent of the model.

Four board reality checks

Boards should demand evidence, not assurances:

1. Who owns each consequential agent’s identity, authority, and revocation capability?
2. Can management compare granted authority with actual actions and exceptions?
3. When was a critical service last restored from a trusted baseline without relying on AI or automation?
4. How are low-risk automated decisions sampled and tested for false negatives?

AI does not make governance obsolete; it makes it operational. Match autonomy with accountability, access with constraint, automation with observability, and deployment with rehearsed recovery. Essentially, Unpredictable does not mean unpreparable.

Dr. Andre Gholam's Words

Beyond Borders: Strengthening Cyber Resilience Through Unified Governance

Cyber threats need no passport. Our governance frameworks still do. Closing that gap may be the defining security challenge of this decade.

The Day the Screens Turned Blue

On 19 July 2024, a faulty CrowdStrike update crashed some 8.5 million Windows devices. Airports, hospitals and banks stalled worldwide, with no attacker involved. If one defective file can do that, imagine a determined adversary. The threat is growing: in the WEF Global Cybersecurity Outlook 2026, 94% of leaders call AI the biggest force reshaping cyber risk. Prevention alone is no longer enough; the goal is resilience: absorbing the blow, staying operational and recovering fast. The message is difficult to ignore: an organization can be secure and still not be resilient.

From Cybersecurity to Cyber Resilience

Cybersecurity traditionally asks: How do we protect ourselves? Cyber resilience asks a broader question: How do we anticipate, withstand, recover from and adapt to an attack—especially when the disruption originates outside our boundaries?

This is where governance becomes fundamental. Technology provides controls; governance defines



accountability, risk appetite, priorities, incident escalation and recovery decisions. NIST CSF 2.0 illustrates this shift by adding "Govern" to Identify, Protect, Detect, Respond and Recover, positioning cyber risk within enterprise governance rather than solely as a technical function. Europe went further: NIS2 makes management bodies personally accountable for cyber risk. But governance within one organization is no longer enough. Why Unity Beats Solo Networks are shared, and so are vulnerabilities. One flaw in a widely used component can travel through thousands of supply chains overnight. Solo initiatives protect a territory; attackers target the whole system. Unified governance offers

what no country can build alone: common definitions, one incident report instead of ten, faster cross-border evidence sharing, trusted channels in a crisis and pooled capacity for nations that cannot afford elite defenders.

The proof is in the results: in February 2024, Operation Cronos, led by the UK's National Crime Agency with partners in ten countries, dismantled LockBit, then the world's most prolific ransomware group. No single agency could have done it alone.

Why "Unified" Governance? Unified governance should not mean a single worldwide regulator or identical legislation everywhere. Countries differ in legal systems, sovereignty, economies and cyber maturity. Rather, it means interoperable governance: shared principles, compatible minimum requirements, common terminology, trusted information exchange, coordinated response and mutual assistance.

The Price of Fragmentation Fragmentation itself becomes a vulnerability: inconsistent security requirements, conflicting reporting obligations, duplicated compliance and uneven cyber maturity.

Most importantly, fragmented governance creates a dangerous mismatch:

attackers operate globally while defenders may still be organized locally.

We are not Starting from Zero

Several initiatives already provide pieces of a future collective governance model.

At organizational level, NIST CSF 2.0 provides an outcome-based cyber risk framework.

Regionally, the EU's NIS2 Directive creates a common cybersecurity framework across 18 critical sectors. The EU Cyber Solidarity Act, in force since February 2025, goes further toward collective resilience. ASEAN's Cybersecurity Cooperation Strategy 2026-2030 strengthens regional collaboration in incident response, CERT coordination, capacity building and cybersecurity policy. Internationally, the Budapest Convention on Cybercrime, with 82 parties, supports cybercrime legislation and international cooperation, while the UN Global Digital Compact (2024) promotes a safe and secure digital future through global cooperation.

The UN Convention against Cybercrime (2024) marks another milestone: 82 countries supported it, but only 3 had ratified it by September 2026—showing that global agreement must lead to implementation. From Islands of Resilience to an Ecosystem of Trust The challenge, therefore, is not the absence of frameworks. It is how to make them converge rather than compete.

Future cyber resilience

requires governments, regulators, businesses, technology providers, international organizations, academia and civil society to share responsibility without losing accountability. Harmonized principles, cross-border threat intelligence, common incident taxonomies, coordinated exercises, mutual assistance and capacity building can turn isolated defenses into collective resilience. Perfect global uniformity may neither be realistic nor desirable. Interoperability may be the more achievable objective: different governance systems capable of speaking the same cyber language when it matters most.

We have moved from protecting computers to organizations, then to digital ecosystems. The next step may be from fragmented to shared resilience.

Will the world ultimately achieve truly unified cyber governance?

Only time will tell. But cyberspace will not wait for us to decide.





THE URAEUS | PROTECTION CYBERSECURITY

ANCIENT SYMBOL — THE URAEUS

The Uraeus, represented as the raised cobra, was associated with royal authority and protection. Its upright posture creates an immediate visual impression of alertness: ready to detect danger and defend what it protects.

THE MODERN CONNECTION — CYBERSECURITY

That idea translates naturally into cybersecurity, where protection depends on constant vigilance. Modern organizations operate within interconnected digital environments where threats can be invisible, distant, and constantly changing.

The Uraeus becomes a metaphor for the organization's digital defense system — monitoring networks, identifying threats, protecting information, and creating barriers between critical assets and potential attacks.

Its raised hood can therefore be reimagined as a modern digital shield: a protective perimeter that is always watching.

THE PRINCIPLE

“PROTECTION BEGINS WITH VIGILANCE.”

Cybersecurity is not only about responding when something goes wrong. It is about continuously detecting, anticipating, and defending against what may happen next.

Thokoziile Kuwali's Words

Beyond Transition: One Year of the Global Internal Audit Standards, Are African Internal Auditors Delivering Public Value?

The 2024 Global Internal Audit Standards (GIAS), issued by The Institute of Internal Auditors (The IIA) on 9 January 2024 and effective from 9 January 2025, marked an important milestone for internal auditing. The Standards provide a global basis for quality and effectiveness while strengthening internal audit's contribution to governance, risk management and control. The one-year transition period was intended to help functions understand requirements, assess readiness, identify gaps and prepare for implementation. One year on, the key issue for Africa is whether the transition is translating into stronger quality, credibility and impact.

The GIAS define internal auditing's role in strengthening governance, risk management and control while recognising its contribution to organisational stability, sustainability and the public interest. Internal audit provides assurance, advice, insight and foresight across operational efficiency, reporting, compliance, asset safeguarding and ethical culture. For public and private institutions, this supports good governance, accountability and compliance.

The importance of this role is heightened by Africa's changing environment. The



continent's population has grown from approximately 366 million in 1970 to an estimated 1.6 billion in 2026, increasing demand for healthcare, education, housing, water, sanitation, energy, transport and social protection. Governments must meet these needs while managing constrained resources, complex risks and rising expectations for effective public services. Strong governance, risk management, reliable information and accountability are therefore essential to delivering value to citizens.

Readiness remains an important issue. Research conducted at the end of 2025 found that 40% of respondents were only somewhat familiar with

the new Standards at implementation, while another 20% were not yet prepared to begin implementation. These findings show that a global framework does not automatically create readiness. Awareness, technical competence, resources, leadership support and practical implementation mechanisms are needed to turn the Standards into effective practice.

Quality is central to this process. Principle 12, Enhance Quality, places continuous improvement and quality assurance at the centre of internal audit. Boards, audit committees, management and regulators need confidence that internal audit work is objective, evidence-based, relevant and reliable. Where competence, resources, independence or understanding are insufficient, stakeholder reliance can be weakened.

The public-interest dimension is equally important. Weak procurement controls, ineffective project management, poor asset management, unreliable information and inadequate risk management can contribute to delayed infrastructure, inefficient services, financial losses and reduced public confidence. Internal audit therefore has a role beyond identifying weaknesses: it can help

institutions understand and manage risks that threaten strategic and public-interest objectives.

Africa's development trajectory also makes sustainability a governance and risk issue. Population growth, urbanisation, technological change, climate-related risks, infrastructure needs and rising service expectations are occurring alongside resource constraints. Internal audit increasingly needs to understand strategic, operational, technological, environmental and social risks and assess their impact on organisational objectives. This aligns with the African Union's Agenda 2063, which emphasises inclusive growth, sustainable development, good governance and capable institutions. The GIAS cannot deliver these objectives on its own, but it provides a professional framework for strengthening institutional governance, risk management and control.

Implementation should not be measured only by whether a function has amended its charter, updated its methodology, revised its audit manual or completed a standards-mapping exercise. These steps are necessary, but not sufficient. The more important question is whether implementation is changing how internal audit operates and whether stakeholders can see improvements in quality, relevance and impact. Conformance should be the foundation, quality the objective and public value the ultimate contribution.

African internal audit functions face uneven awareness and preparedness, differences in professional capacity, resource constraints, limited specialised skills, technology gaps and varying organisational maturity. Public-sector functions may also face challenges related to legal mandates, funding and institutional structures. Addressing these gaps requires cooperation among professional institutes, boards, audit committees, regulators, academic institutions, chief audit executives and senior management.

At the same time, the GIAS provide a common global language and an opportunity to reposition internal audit around quality, effectiveness and value. They can strengthen governance and accountability while encouraging functions to engage beyond traditional compliance with emerging risks, sustainability, digital transformation, strategic objectives and long-term resilience.

One year into implementation, Africa's internal audit profession is at an important point of reflection. The transition should not be viewed as a destination reached on 9 January 2025, but as the beginning of a continuing journey. The profession must assess investment in knowledge, skills, resources and implementation support and identify remaining gaps.

Ultimately, the success of the Standards will not be demonstrated by the number of functions completing an implementation checklist. It will be demonstrated when boards and management have greater confidence in internal audit, stakeholders rely on its assurance and insight, risks are addressed proactively, governance is strengthened and institutions are better able to achieve their objectives.

For Africa, this opportunity is larger than technical compliance. A rapidly growing population, constrained resources, rising public-service expectations and sustainability pressures require institutions that are capable, accountable and resilient. Internal audit can contribute by strengthening governance, risk management and control.

One year on, the key question is no longer simply, "Have we implemented the Standards?" It is: "Have we built the capability and quality necessary for stakeholders to trust and rely on internal audit as Africa strengthens its institutions, improves public services and pursues sustainable development?" The answer will determine whether the first year of the GIAS remains a transition period or becomes the beginning of meaningful transformation and value addition.

Sami Rifky's Words

The Human Element in Cybersecurity: Behavioral Issues and Implications

Cybersecurity is often presented as a technology issue. Organizations invest in firewalls, endpoint protection, identity management, monitoring tools, or artificial intelligence. These controls are important. But technology alone is not enough. Behind many cyber incidents, we still find a human action. An employee clicks on a phishing link. A manager approves an urgent request without checking it. A user chooses an easy password. An administrator ignores an alert after receiving too many. The human element should be managed as a real risk dimension, not only as an awareness topic. Understanding why people make security mistakes. With optimism bias, a person may understand the threat of phishing but still think: "It will probably not happen to me." This attitude can reduce vigilance. Authority bias can lead an employee to act on an urgent email apparently coming from the CEO, CFO or IT department before verifying it. Cybercriminals use this behavior to bypass good technical controls. Decision fatigue also matters. Employees manage passwords, MFA requests, warnings and access approvals. When security becomes too complicated, users look for shortcuts. Sometimes, the problem is not that employees do not care about cybersecurity. The process itself may be too

GRC Egypt Magazine

difficult to follow. Social engineering targets the person, not the system. Poor language and unusual email addresses are no longer enough to identify phishing attempts. Generative AI can help attackers write more personalized messages. Deepfakes can imitate voices and images. Information on professional and social networks can make a false story more convincing. It can be easier to convince an authorized person to open the door than to break a technical control. Employees should question unusual situations, not only suspicious emails. An urgent request from a senior manager, a change in bank details, an unexpected MFA notification, or a request for confidential information should trigger verification. From awareness training to behavioral security. Most organizations provide awareness training. The question is whether it changes behavior. One annual course is not enough. Employees may repeat the same mistake months later. Training should be continuous and practical. Short awareness messages, phishing simulations, realistic exercises and role-specific training can help. Finance employees face different risks from IT administrators or HR employees. Training should reflect this. Employees should feel able to report mistakes. If someone clicks on a suspicious link, the



ISACA Accredited Trainer
Vice-president and Immediate
Past President of ISACA
Casablanca Chapter

priority is to report it quickly and contain the incident. A culture based only on blame can encourage people to hide mistakes. The objective is not to create perfect employees. It is to make secure behavior easier and ensure that mistakes can be detected and corrected rapidly. Technology can also help the human. Technology should compensate for predictable human limitations. Multi-factor authentication can reduce the consequences of stolen passwords. Privileged access management can limit excessive rights. User and Entity Behavior Analytics can identify unusual access to sensitive information or connections from unexpected locations. AI can also help detect behavioral anomalies. These tools should complement human judgment, not replace it. Zero Trust follows a similar principle. Being inside the network should not

automatically make a user trusted. Access should depend on identity, context and actual need, rather than implicit trust.

A GRC issue, not only a cybersecurity issue

Governance should define responsibilities and expected behaviors. Risk management should identify human-related scenarios and assess their impact. Compliance should ensure that required controls and training are implemented. Internal audit should assess whether these mechanisms work, rather than only checking that policies and training exist.

Organizations can monitor phishing simulation results, repeated authentication failures, reporting rates for suspicious emails, privileged access exceptions, and recurring policy violations.

These indicators should help management improve processes, controls and security culture, rather than simply measure employees.

Conclusion

Human behavior cannot be completely standardized, making human risk difficult to manage. Calling people the “weakest link” is too simple. Employees can create vulnerabilities, but they are also an important line of detection and defense.

Organizations should combine people who understand the risks, processes that make secure behavior easier, and technology that limits the consequences of human errors.

Cybersecurity becomes stronger when it reflects real human behavior, rather than assuming that people will always act exactly as policies expect.





**A NEW STORY
IS ABOUT TO UNFOLD.**

ARE YOU READY?



WATCH

LEARN

GROW

Don't just follow the conversation.
Become Part Of It.

GRCEED

Learn from
the Summit

GRC
SUMMIT EG

WhisperBox

Conversations
Beyond
the Stage

GRCAST

Hear the Voices
Behind the Ideas

SUBSCRIBE

@GRC SUMMIT EG

THE DJED

STABILITY

COMPLIANCE

ANCIENT SYMBOL — THE DJED

The Djed is associated with stability, endurance, and permanence. Its strong vertical structure and repeated horizontal elements create a visual language of something firmly established and capable of standing over time.

THE MODERN CONNECTION — COMPLIANCE

Compliance provides a similar foundation within modern organizations. Regulations, policies, standards, procedures, and controls establish consistent boundaries for how an organization operates.

The Djed therefore becomes a metaphor for the stable framework created by compliance. Its repeated structure represents consistency; its vertical strength represents standards that support responsible decision-making.

Rather than seeing compliance as simply a collection of rules, the Djed presents it as the structure that allows an organization to operate with consistency, integrity, and confidence.

THE PRINCIPLE

“STABILITY COMES FROM STRUCTURE.”

Strong organizations do not leave integrity to chance. They build standards into the systems that guide their decisions and actions.



Hatem Aziz's Words

Why KYC Matters: More Than Just Compliance

When people hear the term KYC, or "Know Your Customer," the first things that usually come to mind are regulations, compliance, money laundering, and financial crime. These are important reasons why KYC has become an essential part of modern business, particularly in financial services. But KYC is about more than compliance.

At its core, KYC is about understanding the customer: who they are, what they need, and how a business can provide products or services that are appropriate for them.

The idea of knowing your customer is not new. Long before KYC became associated with regulations and compliance requirements, businesses naturally needed to understand the people they dealt with. A good businessperson has always tried to understand a customer's needs before deciding what to offer.

Consider a jeweler. When a customer walks into a jewelry shop, the jeweler may want to understand the occasion, the customer's preferences, and perhaps their budget. This helps the jeweler decide whether to show everyday

commercial jewelry, something more exclusive, or a high-end diamond piece.

The same applies to a car dealer. A salesperson may ask what car the customer currently drives, what they are looking for, how they intend to use the car, and what budget they have in mind. The objective is not simply to sell the most expensive car, but to understand the customer well enough to recommend a vehicle that suits their needs.

This principle also applies to marketing and customer segmentation. Imagine a company advertising a villa priced at 15 or 16 million Egyptian pounds. The advertisement may be excellent, but its effectiveness depends greatly on where it is placed. If it is shown to people who are unlikely to be interested in, or able to afford, the property, the marketing effort is not reaching the right audience.

Understanding customers allows businesses to identify different customer groups and offer products and services that are relevant to them. In this sense, KYC information can become more than a compliance



Chief Compliance Officer of
Commercial International Bank

record; it can support better business decisions and a better customer experience.

The same principle is particularly important in banking. Banks and other financial institutions deal with customers who may have very different income levels, sources of wealth, businesses, transaction patterns, and financial needs. A proper KYC profile helps the institution understand who the customer is and what kind of activity would normally be expected from them.

For example, if a customer's transactions are significantly different from what would normally be expected based on their stated profile, this may raise a question that needs to be understood. It does not automatically mean that something is wrong. It may simply mean that the

customer's circumstances have changed and that the institution needs to understand why and, where appropriate, confirm the legitimate source of funds.

This is why KYC should not be treated as something that happens only once, when an account is opened. Customers change. Businesses grow or decline, income and wealth change, and economic and market conditions can affect a customer's financial position. KYC information therefore needs to be reviewed and updated appropriately so that it continues to reflect the customer's circumstances.

The development of modern KYC has also been strongly influenced by financial regulation and the growing focus on preventing money laundering, terrorist financing, fraud, and other forms of financial crime. Over time, regulatory requirements have given KYC a more formal structure, requiring institutions to identify customers, understand their activities, assess relevant risks, and maintain appropriate records.

However, if KYC is viewed only as a regulatory requirement, part of its broader value can be missed. Compliance gives KYC structure, while understanding the customer gives it practical business value.

Today, technology is creating another important chapter in the development of KYC. Electronic KYC, or e-KYC, and digital identity solutions are making customer onboarding faster and more convenient. Customers can increasingly establish their identity and access services without visiting a branch or meeting an employee face to face.

But this convenience creates a new challenge: how do we know that the person behind the screen is really the person they claim to be?

The challenge is not limited to the person. It also applies to documents presented digitally. If a customer provides an identity document electronically, how can an institution determine that the document is genuine, has not been manipulated, and actually belongs to the person presenting it? What standards should determine whether a digitally presented document can be accepted as reliable evidence of identity?

Technologies such as biometrics, facial recognition, liveness checks, digital identity systems, and document verification can provide additional layers of assurance. However, technology does not remove the need for reliable verification standards. It changes how verification is performed and creates new questions about trust, reliability, and the quality of the evidence being used.

This brings KYC into a new phase. The challenge is no longer only to collect information about a customer, but also to establish and verify that information reliably in an increasingly digital environment.

Ultimately, KYC is a combination of understanding, verification, and ongoing awareness of the customer. Regulation has given it an important formal framework, while technology is changing how it is performed. But the underlying principle remains simple: a business needs to understand who it is dealing with in order to serve that customer appropriately and responsibly.

Ihab Kamel's Words

Clarity Is a Strategic Advantage

In business, the challenge is often not a lack of information, but an excess of it.

Executives today operate in an environment filled with meetings, reports, emails, dashboards, competing priorities and constant opinions. Yet more information does not necessarily lead to better decisions. In many organizations, it can create the opposite effect, more activity, slower decision-making and less focus on what truly matters.

Strong executives develop the discipline to distinguish between what is urgent and what is important, between operational activity and genuine value creation, and between useful information and unnecessary noise.

This discipline becomes even more important at board level.

A board should not become absorbed in the day-to-day detail of the business. Its responsibility is to step back, challenge assumptions and focus management's attention on the issues that materially influence value, risk, performance and long-term direction.

Consider capital allocation during a transformation.



Management may present several attractive investments, expansion opportunities and operational initiatives, each supported by detailed analysis. The board's role is not simply to review every proposal, but to ask the fundamental questions: Which investments create the greatest long-term value? What should be prioritized now? What can wait? And what risks are we prepared to accept?

Clarity also improves accountability. When strategic priorities are clearly defined, management understands what matters most, resources can be allocated more effectively and performance can be assessed against

meaningful outcomes rather than activity alone.

The same principle applies during periods of uncertainty. Complexity often encourages organizations to add more reports, more meetings and more layers of decision-making. Effective leadership frequently requires the opposite, simplifying the agenda, identifying the few decisions that matter most and ensuring that the organization remains aligned around them.

Clarity does not mean oversimplifying complex issues. It means understanding complexity well enough to identify what is truly important.

When the noise is removed, priorities become clearer, decisions become sharper and governance becomes more effective.

In an increasingly complex business environment, clarity is more than a communication skill.

“It is a strategic advantage.”

Tarek El Rayes's Words

AI Resilience: Governing the Technology, Empowering the Human

Artificial Intelligence is transforming cybersecurity. It enables organizations to detect threats faster, analyze vast amounts of data, automate repetitive activities, and strengthen decision-making. Yet, as AI becomes more deeply embedded in our organizations, a fundamental question emerges: How do we remain resilient when our dependency on AI increases? The answer goes beyond technology. It lies in AI governance and human resilience. AI can analyze, recommend, prioritize, and automate. but people remain accountable for the decisions that matter. As organizations adopt AI across cybersecurity, risk management, compliance, and business operations, human oversight becomes more, not less important. People must understand when to trust an AI output, when to challenge it, and when to intervene. This makes AI governance an organizational responsibility, not simply a technology initiative. Effective governance requires clear ownership, defined accountability, appropriate security and privacy controls, human oversight, and

clear boundaries around what AI can decide or execute. Cybersecurity must be embedded within this framework. Organizations need to understand how AI systems access data, interact with critical platforms, and introduce new security, operational, privacy, and third-party risks. True resilience also means preparing for failure. Organizations should conduct AI-focused tabletop exercises to explore scenarios such as an AI system producing an incorrect recommendation, an AI agent being compromised, sensitive information being exposed, or a critical AI capability becoming unavailable. These exercises should test more than technology. They should bring together people, processes, technology, governance, and crisis management, while clarifying when AI can act, when human approval is required, and how accountability is maintained. Ultimately, AI should not replace human responsibility; it should augment human judgment. The resilient organization of the AI era will not simply be the one that adopts the most advanced technology. It will be the one that can



CISO FAB MISR- Information Security,
BCM & Data Privacy

govern AI responsibly, secure it effectively, prepare for its failure, and empower its people to work confidently alongside it. The future of cybersecurity is therefore not human versus machine. It is human judgment augmented by intelligent technology, supported by strong governance and a culture of resilience. In the age of AI, trust must be engineered, responsibility must remain clear, and resilience must remain human.

Engy Metwally's Words

When Governance Becomes a Growth Engine

For years, governance has often been perceived as the part of the organization that says “no”: more approvals, more controls, more documentation and, sometimes, more bureaucracy.

After more than two decades working across audit, compliance, governance, strategy and transformation, my experience has taught me the opposite. Good governance should help the business move faster, not slower. Poor governance creates hidden friction. It appears in unclear decision rights, repeated discussions, unnecessary escalation, manual workarounds and decisions being pushed upward simply “to be safe.” I have seen situations where the business was ready to move, yet progress was delayed because it was not clear who had the authority to decide, who needed to be consulted or what level of risk was acceptable. Whether approving a commercial exception, entering a partnership or launching a new initiative, the solution is rarely another approval layer. It is clearer authority, stronger accountability and better risk visibility.

For me, good governance creates four things: clarity, confidence, speed and sustainable growth. Clarity defines who decides and when escalation is required. Confidence allows leaders to delegate. Speed follows

when decisions stop travelling through unnecessary layers. Growth becomes sustainable when processes, controls and responsibilities can scale with the business.

The same principle applies to operations. A process may technically “work” while depending heavily on spreadsheets, emails, individual judgment or one experienced employee who knows how everything fits together. That may work today, but it quickly becomes a constraint when the organization grows, leadership changes or technology is introduced. Internal Audit adds its greatest value not by adding another control, but by challenging why the workaround exists in the first place.

AI is perhaps the clearest test of this thinking today. Organizations want employees to experiment, automate work and develop new use cases, and the reality is that adoption is already happening. Simply restricting access will not stop it; it may only drive it underground and create “shadow AI.” Yet unrestricted use creates equally serious risks around confidential information, intellectual property, accuracy, accountability and decision-making.

The answer is not AI or governance. It is AI with governance. That requires more than issuing an AI policy. Organizations need to define which tools are approved,



Chief Audit & Compliance Officer

what information can and cannot be shared, when human validation is mandatory, who is accountable for each use case, and how applications should be classified based on data sensitivity and business impact. Low-risk productivity uses should be allowed to move quickly, while higher-risk applications should receive stronger review and oversight. This is what proportionate governance should achieve: guardrails that enable innovation, not roadblocks that suppress it. Modern GRC therefore needs to move beyond asking only, “What could go wrong?” We must also ask, “How can we enable the business to move forward with clarity, confidence and informed risk-taking?” Governance should not be measured by the number of controls introduced, but by whether the organization can make better decisions, take informed risks, innovate responsibly and execute with confidence. When governance achieves that, it is no longer the brake on growth. It becomes part of the engine.

Yasmin El Gibaly's Words

Internal Audit impact on GRC to strengthen Business Decision-Making

In today's business environment, organizations are making decisions faster than ever. Markets change drastically based on changes in customer expectations as impacted by Digital transformation, cybersecurity and artificial intelligence leading to new emerging risks. In this environment, Governance, Risk and Compliance (GRC) is no longer simply a control mechanism—it is becoming an essential enabler of better business decisions. Internal Audit plays a distinctive role within this ecosystem. While management owns risks and makes business decisions, Internal Audit provides independent and objective assurance over whether governance, risk management and control processes are designed and operating effectively before risks materialize into costly consequences. From hindsight to foresight: Traditional Internal Audit has often been associated with reviewing historical transactions and identifying control gaps. Internal Audit is currently moving toward a more forward-looking approach through analyzing risk trends, emerging threats, control data, regulatory developments and business performance indicators.

Internal Audit helps ensure that the decision-making mechanism is well designed and operative to provide a clearer view of the risk, opportunity, assumptions and potential consequences surrounding the business decisions. Data analytics, continuous monitoring and emerging technologies can further strengthen this capability by enabling Internal Audit to identify patterns and anomalies earlier, allowing management to respond earlier before issues escalate. The greatest opportunity for Internal Audit lies in not only helping management rectify the issues but also help them understand the impact of those issues on the organization as a whole, what objective they could affect, and where similar vulnerabilities may exist across the organization to be avoided. Accordingly, Internal Audit adds significant value in ensuring that the risks are properly mitigated and the opportunities are appropriately optimized while complying with the market regulatory requirements.



Chief Audit Executive of
Industrial Development Bank

This creates an important aspect as in: Business takes the leap for expansion and growth while the Internal Audit acts as the safety net to keep its growth sustainable and secured. The future of Internal Audit is therefore not simply about asking, "Did we get it right?" It is increasingly about helping the organization ask, "Do we have the right mechanism to support strategic decisions?"





THE SCALES OF MA'AT

| BALANCE AUDIT

ANCIENT SYMBOL — THE SCALES OF MA'AT

The scales associated with Ma'at represent the ideas of balance, truth, and judgment. They embody the principle that what is presented can be measured against a standard.

THE MODERN CONNECTION — AUDIT

This creates a direct conceptual connection with audit. At its core, audit examines the relationship between what should happen and what actually happened.

Expectation is compared with reality.
Claims are compared with evidence.
Risk is considered alongside control.
Performance is examined against accountability.

The scales therefore become a visual metaphor for the process of examining, measuring, and verifying.

THE PRINCIPLE

“EVERY BALANCE TELLS A STORY.”

Audit turns information into insight by revealing where reality aligns with expectations — and where the gaps begin to matter.

Mohamed Abdelmalek's Words

The UAT Illusion: Why Banking AI Breaks Traditional Governance

The traditional IT comfort.

Ask any banking executive how enterprise software works, and they will describe a predictable rhythm: you gather requirements, build the application, test it thoroughly in User Acceptance Testing (UAT), and deploy it. Once live, a core banking platform or payment switch behaves with mechanical certainty. If it passed UAT on Friday, it will deliver the exact same outcome on Monday -- and for the next ten years.

The ingrained blind spot.

We grew comfortable with this mental model over decades. But when applied to Artificial Intelligence, it quickly becomes a dangerous blind spot.

The consumer chatbot

misconception. Leadership often views AI through the lens of popular public chatbots, assuming it is plug-and-play software. It is not. Traditional applications follow rigid, deterministic rules; AI operates on statistical probabilities. An AI model is not a static piece of machinery you install -- it is a living organism.

The reality of model drift.

A credit-scoring or fraud algorithm can pass every UAT milestone with flying colors. Yet months into production,



as economic realities or customer behaviors shift, the model quietly 'drifts.' Without anyone touching a single line of code, it begins making erratic loan decisions or developing discriminatory biases. In AI banking, Go-Live is not the finish line; it is day one of risk.

"In traditional banking IT, Go-Live marks the end of risk. In banking AI, Go-Live is merely day one of operational exposure."

The limits of legacy

committees. Crucially, bank leadership must recognize that AI governance cannot simply be handed to the CRO as another agenda item for the monthly risk

committee. Legacy risk frameworks were built for human time: change-advisory boards with one-week lead times, risk assessments with 48-hour SLAs, and quarterly committee reviews.

The velocity mismatch. AI operates at machine speed. When an autonomous model approves credit or executes transactions in milliseconds, a model failure does not wait for next Tuesday's committee. If an algorithm drifts off course, waiting days for an operational risk review means thousands of erroneous decisions and immediate regulatory or reputational damage.

A new operational reflex.

Governing enterprise AI requires fresh organizational muscle: dedicated multidisciplinary AI Governance Committees, algorithmic 'circuit breakers' (automated kill-switches), and real-time operational risk triage protocols that can intervene within minutes, not weeks.

The boardroom mandate.

Before approving your next AI budget, ask your leadership team: Are we prepared to govern an asset that never stops evolving, at a speed our current committees were never built to handle?



Empowering ambitions today & enabling possibilities for generations to come

At Commercial International Bank (CIB), we build on a long legacy of trust and performance, and every moment is an opportunity to create lasting value as we help build the next era of prosperity. With a deep understanding of our world, we move forward with purpose, driving progress through trust and expertise at every step.

GLOBAL
FINANCE

EGYPT



Abdelmonem Hany's Words

Deepfake Video Fraud: Can You Trust the Face on Screen?

Your boss calls you on video. Nothing seems off. You recognize the face, the voice sounds right, they bring up a project you've been working on. Then comes the ask: approve an urgent payment. Would you stop and check first? Honestly, most people wouldn't. And that's exactly the gap deepfake fraud is built to exploit.

With advances in recently developed artificial intelligence (AI) methods, crafting fake audio and video recordings of high quality is now easy for almost anyone. Generative AI methods, created for entertainment, such as synthesizing paintings or music, have also been turned toward good and bad uses; some AI programs can create high-quality fakes that appear like normal images, audio, or video, presenting people speaking in any language while mimicking their appearance and voice. The term deepfake fraud refers to video fraud employing AI-generated media where a perpetrator maliciously misuses or misrepresents an individual's appearance or voice to deceive another person or entity for monetary gain. In Hong Kong, an employee transferred roughly HK\$200 million after attending a video conference that turned out to be entirely fabricated — prerecorded footage of people who were never actually on the call. The official government account lays out what happened. The

meeting was fake. The money was not.

We've been trained to treat video calls as proof. Seeing a face feels more reliable than reading a message — it's just how we're connected. But AI can now change how someone looks and sounds well enough that the "familiar face" test doesn't work anymore. It's not always a live performance, sometimes it is prerecorded tape passed off as a live meeting. Other times there is an actual person on the call, just with their face swapped. Criminals don't need perfect technology — they just need something convincing enough to catch you for thirty seconds.

What makes this work is not only the technology — it's the pressure around it. A request from someone who looks like your manager carries built-in authority. A tight deadline makes you not want to ask questions. And if you're told to keep it quiet, you might not loop anyone else in even when something feels uncomfortable. None of that makes someone innocent. It just means the scam is counting on habits that are normally useful (but not always) trusting coworkers, moving fast, wanting to help. This is not only a corporate related risk, but people also face the same scam in online relationships and investment — build trust with a convincing video call, then ask for money. Above all else, deepfake technologies have the potential to not only present



Head of Audit Quality Assurance and Improvement program

as significant risk but also have the potential to be used in a way that undermines the integrity of information shared and communicated over the internet. Hence, it is most prudent for organizations to have layered defense aimed at deepfake technologies. The best defense strategy for organizations to prevent such a threat is to implement comprehensive security awareness training to help their employees with recognizing and understanding how these technologies can impact their personal and work lives. Adequate training should help to build a culture of verification and encourage staff to double check suspicious requests. This should also be supplemented with periodic team exercises and realistic simulations to convey the training messages and provide practical direction on how to identify malicious initiatives.

Detecting a deepfake video rather than preventing does not eliminate the potential damage. Therefore, organizations must prepare response and recovery plans as part of their overall incident response management and enterprise risk management approaches. A broader fraud response plan that addresses more than just deepfake videos improves response and recovery capabilities.

Finally, what are the red flags of Deepfake videos?

There are some signs — unusual facial movement, shadows that doesn't quite match, audio that's slightly out of sync with the mouth. But a bad connection can cause the same glitches on a real call. And a smooth, high-quality video doesn't guarantee anything either. Searching for fake indicators in every call is a losing game.

The better move is simpler than spotting a fake: just pause and verify separately. Call the person back on a number you already have saved — not one they gave you during the call. If it's a company, go through whatever contact channel you already know is legitimate. Taking sixty seconds to double-check costs you almost nothing, even if the person on screen seemed completely real.

At work, that means payment verification steps should apply no matter who's asking — even if it looks like the CEO on the call. People need to feel safe pushing back on an unusual request without worrying it'll cost them their job. Families can set up something similar: agree in advance that any surprise request for money gets a callback first, no exceptions.

You don't have to stop trusting video calls altogether. Just treat a big or unusual request as a reason to double-check — not as something to act on immediately because the face looked right.



Amal Ahmed Eweis's Words

Assessing Technology Risk When Banks Build, Buy, or Integrate New Solutions

The banking industry is experiencing a profound transformation. Technology is no longer simply an enabler of banking operations; it has become an essential component of the business model itself. Mobile banking, artificial intelligence, cloud computing, application programming interfaces (APIs), data analytics, digital payments, robotic process automation, and third-party platforms are increasingly embedded in the way banks serve customers and manage their operations.

Build, Buy, or Integrate?
Technology is now central to the banking business model, not merely an enabler of it. Mobile banking, AI, cloud computing, APIs, and third-party platforms let banks innovate faster and personalize service, but greater dependence brings greater technology risk. NIST's 2026 Supply Chain Due Diligence Guide frames due diligence as investigating suppliers and products — covering provenance, resilience, and ownership — to support informed decisions. Three Strategic Paths
When adopting new technology, banks generally choose to build, buy, or integrate:

- Build internally offers control but creates full lifecycle responsibility for architecture, security, maintenance, and



eventual retirement. Secure development practices such as threat modeling, code review, and NIST's SSDF are essential to managing this exposure.

- Buy accelerates delivery and access to specialized expertise, but does not transfer accountability. A vendor failure can become a banking service failure, so due-diligence findings must be written into the contract, including data portability, take-over feasibility, and exit terms.
- Integrate connects new solutions to core banking, payment, and identity systems via APIs. A component that is secure in isolation can still introduce significant risk through its interfaces, making

API governance a control priority.

Critical Due Diligence Dimensions

- Artificial Intelligence: governance must address what happens when a model errs, is biased, or is manipulated — particularly where AI influences customer or financial decisions.
- Resilience: Recovery Time and Recovery Point Objectives should be defined and actually tested, since a recovery plan that exists only on paper offers limited assurance.
- Cybersecurity: identity and access management, MFA, monitoring, and incident response must be verified, in line with ISO/IEC 27001 and Basel third-party risk principles.

- Internal Audit: under the IIA's Three Lines Model, Internal Audit independently assesses whether technology risk is managed effectively, without owning the underlying decisions.

Conclusion

Digital transformation is not slowing down. Banks will continue to build applications, acquire technology, integrate platforms, consume cloud services, deploy artificial intelligence, and rely on third-party ecosystems. due diligence grounded in frameworks such as COBIT, ISO/IEC 27001, and NIST SP 800-161 remains the foundation for ensuring digital dependence stays informed, resilient, and sustainable.

Ihab Haggag's Words

The Role of Governance in Effective Debt Recovery and Restructuring

Governance plays a critical role in ensuring that debt recovery and restructuring processes are effective, transparent, fair, and sustainable. It provides the framework through which financial institutions, creditors, borrowers, regulators, and other stakeholders make decisions, manage risks, and resolve distressed debt. Weak governance can lead to inconsistent decisions, inefficient recovery efforts, conflicts of interest, and further financial losses.

1. Accountability and clear decision-making

Effective governance defines the responsibilities of boards, management, credit committees, recovery teams, and external advisers. This ensures that decisions—such as negotiating settlements, restructuring repayment terms, pursuing legal action, or writing off debt—are based on established policies and objective assessments rather than individual preferences. Clear accountability also enables institutions to measure performance and take corrective action when recovery strategies are unsuccessful.

2. Strong risk management and early intervention

Good governance strengthens the identification and management of credit risk. Institutions should monitor early warning indicators such as missed payments, declining cash flows, excessive leverage, or deteriorating business performance. Early intervention allows creditors to address financial difficulties before they become more severe. This increases the possibility of restructuring debt around the borrower's sustainable repayment capacity rather than merely postponing the problem.

3. Well defined & transparent restructuring

Debt restructuring

involves competing interests: creditors seek to maximize recovery, while borrowers require sufficient flexibility to restore financial stability. Governance promotes transparent criteria for assessing restructuring proposals. Important measures include independent assessment of the borrower's financial condition, clear documentation, appropriate approvals, consistent treatment of similarly situated creditors, and disclosure of relevant information. These practices reduce arbitrary decisions and strengthen stakeholder confidence.

4. Conflict-of-interest management

Debt recovery decisions may be affected by personal, commercial, or institutional relationships. Strong governance addresses these risks through segregation of duties, independent oversight, conflict-of-interest policies, and appropriate controls. Independence is particularly important in large or complex restructurings where decisions may have significant financial consequences.

5. Legal and regulatory compliance

Debt recovery and restructuring must comply with applicable laws and regulations, including those relating to insolvency, secured lending, creditor rights, consumer protection, taxation, and data protection. Effective governance ensures that recovery strategies remain legally sound and enforceable. Compliance also reduces litigation, regulatory, and reputational risks that could undermine recovery outcomes.

6. Sustainable restructuring

Governance helps distinguish temporary liquidity problems from fundamentally unsustainable debt. A restructuring should not simply

postpone losses or repeatedly extend credit to borrowers who cannot realistically repay. Objective analysis should consider cash-flow forecasts, business viability, collateral values, repayment capacity, and the borrower's willingness and ability to comply with revised terms. This supports restructuring solutions that have a realistic chance of success.



Banque Du Caire
Head of Debt Recovery & Restructuring

7. Continuous monitoring and follow-up

Governance continues after a restructuring agreement is reached. Creditors should monitor repayment performance, financial covenants, cash flows, collateral values, and compliance with restructuring conditions. Clear escalation procedures should be established so that deterioration in the borrower's position triggers timely corrective action.

Conclusion

Effective governance is a foundation for successful debt recovery and restructuring. It promotes accountability, transparency, risk management, independence, legal compliance, and sustainable decision-making. When applied effectively, governance enables creditors to identify problems early, make objective and well-documented decisions, manage conflicts, and monitor restructuring outcomes. It therefore helps maximize recoveries, minimize losses, protect stakeholder interests, and give viable borrowers a better opportunity to restore financial stability.

THE LOTUS

TRANSFORMATION

ESG

ANCIENT SYMBOL — THE LOTUS

The Lotus was an important symbol in Ancient Egyptian visual culture and was associated with renewal, regeneration, and emergence. Its recurring cycle of appearing from the water and opening toward the light provides a powerful visual metaphor for transformation.

THE MODERN CONNECTION — ESG

This cycle connects naturally with ESG, where organizations are increasingly challenged to rethink how they use resources, affect communities, create value, and prepare for the future.

The Lotus becomes a metaphor for an organization capable of renewing its systems rather than simply maintaining them. Its organic form can evolve into circular economies, sustainable infrastructure, renewable systems, environmental data, and interconnected social networks.

The symbol therefore moves from natural renewal to organizational transformation.

THE PRINCIPLE

“TRANSFORMATION IS THE NEW LEGACY.”

ESG is not simply about reacting to environmental and social challenges. It is about transforming the way organizations create long-term value and impact.



Naglaa Nosseir's Words

From CSR to ESG: A Mandate Governance

For decades, corporate social responsibility spoke the language of generosity. Companies described their contributions through narratives and beneficiary counts, addressing an audience largely outside the organization. ESG has changed the conversation. Impact is no longer a matter of intention but of accountability, and the question has shifted from what we do to how we govern what we do. That shift, more than any framework or rating, is the real transformation facing boards, executives, and practitioners alike. The Governance Shift The first lesson of the CSR-to-ESG transition is structural. CSR traditionally lived in one department, with a budget, a calendar of initiatives, and a public relations function. ESG is a crossfunctional mandate that touches strategy, risk, finance, operations, and people. If impact remains siloed, it cannot be governed. Successful organizations give their sustainability agenda a clear ownership structure: an executive sponsor, a cross-functional committee, and a materiality assessment identifying the issues genuinely material to the business and its stakeholders. The committee's role is not to approve projects but to test their coherence with strategy, scrutinize their risks, and hold owners to account. Progress is reported on a dashboard with the same



discipline as financial performance. Structure precedes substance; without it, even excellent programs remain anecdotes. From National Ambition to Board-Level Targets The second lesson concerns alignment. In Egypt, as in many countries, national development strategies set ambitious goals, from digital transformation to inclusive growth, and expect the private sector to contribute. The governance question is how such ambitions become organizational targets. This demands a deliberate choice of what to measure. Reach is the easiest metric but rarely the most honest: the number of people touched says nothing about whether capabilities changed. Outcome indicators, program sustainability, cost efficiency, and stakeholder trust are harder to measure

and far more revealing. Materiality is the filter: what deserves board attention is what matters to business continuity and stakeholder confidence, not everything labeled social. Boards that accept only vanity metrics are not governing impact; they are curating its image. Risk Is Part of Impact The third lesson is the most neglected: delivering social impact carries genuine risk. Initiatives in underserved areas face operational challenges, from infrastructure gaps and security considerations to logistical complexity and the expectations of communities promised change before. Reputational risk is equally real when an intervention fails or when its benefits do not outlive its funding. Treating impact as risk-free is naive. Managing it with a proper risk register, clear ownership, and honest reporting is what separates professional delivery from charity, and the discipline applied to commercial projects must govern social ones equally, including the courage to stop what is not working. A Regulatory Inflection The shift from voluntary disclosure to regulatory mandate is the cleanest evidence that ESG has moved from narrative to governance. The Egyptian Financial Regulatory Authority's Resolution No. 107 of 2021 and Resolution No. 108 of 2021 require tiered Environmental, Social, and Governance disclosure

together with TCFD-aligned climate-related financial reporting from every company listed on the Egyptian Exchange and from non-bank financial institutions regulated by the FRA. Reporting is phased in by capital tier: Tier 1 entities - issued capital or net equity of at least EGP 100 million - must file annual ESG disclosures, while Tier 2 entities - at least EGP 500 million - must additionally prepare TCFD-aligned climate-related financial disclosures. What was once optional has become a direct board responsibility: structuring the data, ensuring internal controls, obtaining external assurance, and publishing to a defined cadence. The regulator has, in effect, codified the lessons above - committee, materiality, accountable owner, assured reporting are no longer best practices reserved for sustainability-minded leaders; they are the minimum expectation. Organizations that treat the mandate as a compliance line item will produce the disclosure. Those that treat it as a governance moment will build the institutions the disclosure demands. That difference is what separates a passing grade from durable change.

Making Impact Durable The final lesson is about permanence. Programs end; systems persist. Organizations that convert CSR into durable ESG advantage institutionalize what works: impact objectives embedded in strategy, funded in cycles rather than one-off occasions, subjected to internal audit and external assurance, and reported transparently. This is also the path to trust. Investors, regulators, and partners increasingly ask how impact is governed, not merely what it achieves. For boards across the region, the message is clear. ESG is not a reporting exercise; it is a governance discipline that aligns national ambition with organizational accountability, measures what matters, manages risk honestly, and builds institutions capable of lasting change. Leaders who master it will strengthen their organizations, and define what responsible growth looks like in the digital age.



kamal Fayek's Words

Navigating The Evolving Role of Internal Audit in the ESRMS

The role of Internal Audit is continuously evolving, once focused on financial controls & compliance, it is now a critical player in the "Environmental & Social Risk Management System" (ESRMS). A holistic ESRMS must be embedded into the "Enterprise Risk Management Framework" & credit decision-making, enabling management to identify, assess, manage, monitor, & report E&S risks. This evolution is reshaping Internal Audit vision, Auditors need to be well versed of E&S issues, climate-related risks, Human Rights, Stakeholders' Engagement, & Third-Party Risk.

Embracing The New Regulatory Challenge
On June 30, 2026, The CBE has circulated robust guidelines for implementing ESRMS by January 2028, thus elevating a new challenging journey for auditors to ensure proper adherence.

ESRMS Life Cycle (10 steps)

(1)-Governance:

The journey starts with the need to assess the ESRMS Governance & Policy Setup, clear roles, vital capabilities & expertise.

(2)-Grievance:

A disciplined Grievance Mechanism must be in place to handle E&S complaints (e.g. complaints related to community impacts).

(3)- Exclusion



General Manager, Head of Audit Governance, Quality Assurance & Follow-up , Banque Misr Group

The auditor assesses whether the bank's Credit Portfolio captures any prohibited activities (e.g. child labor) against applicable laws & International Financial Institutions exclusion lists (e.g. IFC list).

(4)- Screening:

E&S risks must be assessed (e.g. hazardous waste from a chemical facility).

(5)- Categorization:

The project must be appropriately categorized in line with the Egyptian Environmental Affairs Agency (EEAA)'s classification. The assigned category (being High or Medium or Low risk)

beacons the depth of Due Diligence. (e.g. for High-risk projects, adequate E&S Impact Assessment from the Ministry of Environment or a Certified Environmental Expert will be mandated).

(6)- Due Diligence:

The depth of Due Diligence must be synchronized with the assigned category, covering the client E&S risks.

(7)- ESAP:

Findings from the Due Diligence must be translated into clear Action Plans with defined roles & targets. (e.g. installing a Bag House Filter in a cement factory, by Q2, 2027).

(8)- Financing Documentation:

The financing documentation must diligently articulate all agreed covenants, (e.g. a new land acquisition).

(9)- Monitoring:

Action-plan progress must be closely monitored, otherwise escalation should take place.

(10)- Reporting

Monitoring results must be translated into disclosures, to adequately support management oversight.

Looking Ahead

Throughout the journey, Internal Audit can help turn ESRMS from a "Requirement" into a "Boosting Mechanism" for portfolio quality, sustainability & long-term value creation.

Amir Anwar's Words

The GRC Triangle: Connecting Governance, Risk, and Control to Drive Sustainable Business Performance

Governance, risk, and control used to run as three separate jobs, the board set policy, risk teams kept a register, auditors checked controls. But sustainable performance depends on all three working together where each side needs the other two to hold up.

Governance sets direction: who's accountable, what's acceptable, how decisions get made and by whom.

Risk management looks ahead: spots what could go wrong or go right, and how much it matters.

Control makes it real: the daily discipline that keeps operations inside the lines governance drew.

Drop any one side and the shape collapses: governance without risk insight is flying blind; risk insight without control is a report nobody acts on; control without governance direction is busy work with no purpose.

Why It Matters Now

Governance: Regulators and stakeholders expect clear accountability, who owns which decision, and evidence the board actually oversees it, not just a policy on file.

Risk: Organizations are more complex and interconnected, so a risk in one unit rarely stays contained. Leaders need one coherent enterprise view, not scattered assessments.

Control: It's where intention becomes practice, while weak controls undo whatever governance and risk work put in place.

The Link to Sustainable Performance

Sustainable performance isn't just growth, it's growth that holds up under stress. Each side of the triangle protects that in a different way:

Governance keeps decisions aligned with long-term strategy rather than short-term pressure, so growth today doesn't create a liability tomorrow.

Risk management keeps the organization within its appetite for threats while still capturing opportunities.

Control protects the value that's already been created, preventing the losses, errors, and breakdowns that quietly erode margins and trust.

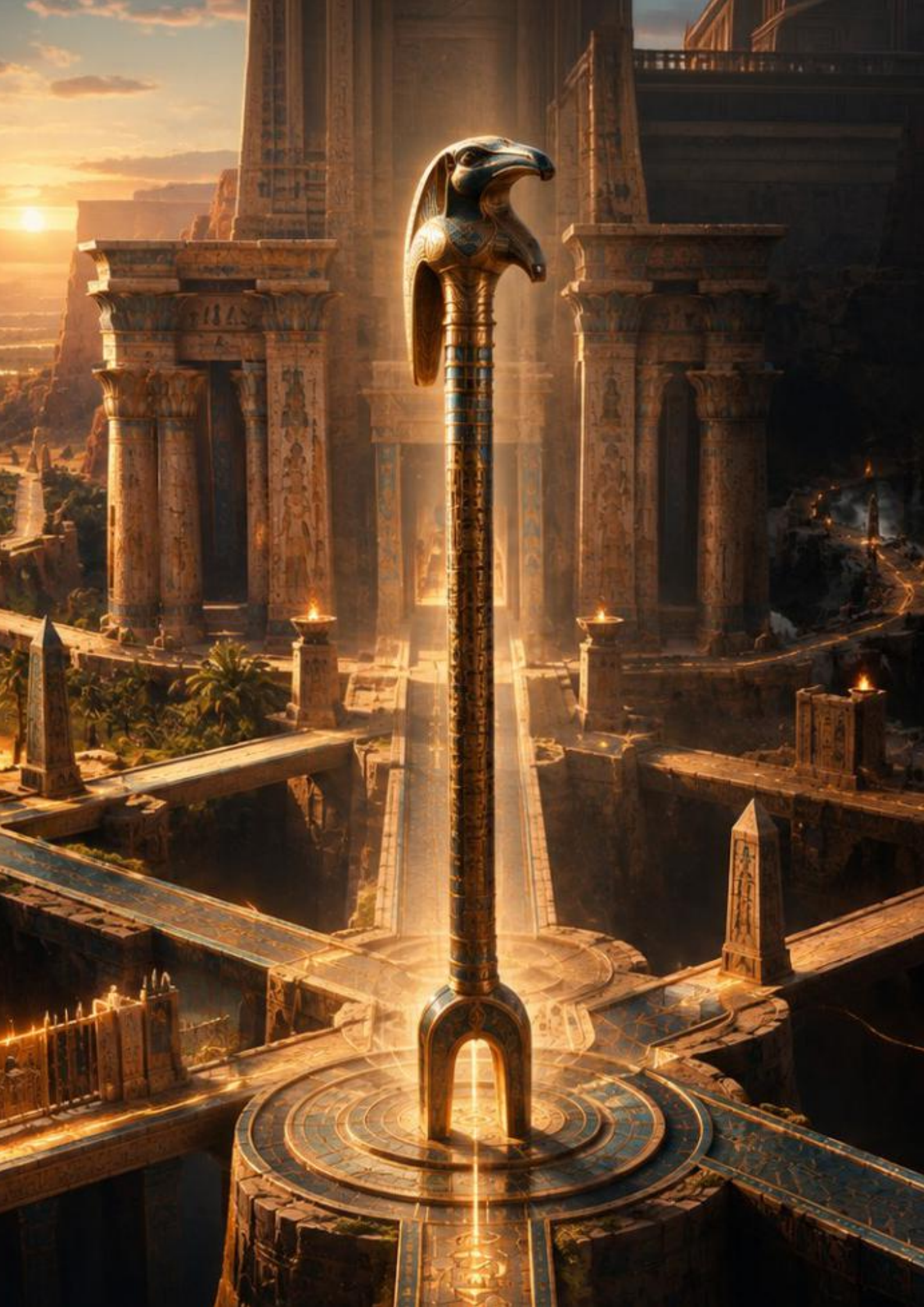
Together, they turn performance from something reactive, chasing results



Group senior director Internal Audit

and cleaning up after surprises, into something durable and repeatable year over year.

The Independent Check Somewhere in the system, someone needs to test whether the triangle actually holds, that direction, insight, and discipline are connected, not just documented separately. That's typically internal audit's role: independent assurance across all three, plus advice on where they're disconnected, without taking over any of the underlying decisions.





THE WAS SCEPTER CONTROL RISK

ANCIENT SYMBOL — THE WAS SCEPTER

The Was Scepter was associated with power, authority, and dominion. Its strong vertical form communicates control and the ability to direct or maintain order.

THE MODERN CONNECTION — RISK

In a modern organization, risk management is fundamentally concerned with understanding uncertainty and maintaining control when circumstances change.

The Was Scepter therefore becomes a metaphor for the systems that help organizations navigate uncertainty: risk identification, assessment, monitoring, controls, mitigation, and preparedness.

Its strong vertical axis represents the stable point around which uncertain conditions can be managed, while branching pathways represent the different directions risk can take.

THE PRINCIPLE

**“CONTROL WHAT YOU CAN. PREPARE FOR
WHAT YOU CAN’T.”**

Risk cannot always be eliminated. But organizations can understand their exposure, establish controls, prepare for disruption, and build the capacity to respond.

■ Mohamed Samir's Words

Internal Audit: From Theory to Practice and the Expectations of the Audit Committee, Senior Management & Regulatory Bodies

In today's financial institutions, Internal Audit can no longer be measured simply by whether it has an annual audit plan and delivers its assignments on time. Its real value goes far beyond completing a plan. It is about trust, governance, resilience, and protecting the institution. Internal Audit is not a function designed to "catch people doing things wrong." It is an essential component of the Governance, Risk and Control framework, providing independent assurance, insight and advice that enable the Board and Senior Management to make better and more informed decisions. The real value of an assurance engagement is not merely identifying a finding. The issue already exists; Internal Audit does not create it. The value comes from understanding the root cause, challenging underlying weaknesses, and helping management develop sustainable solutions that prevent recurrence rather than simply correcting the sample identified during the audit.

This is where the relationship between the Chief Audit Executive (CAE) and Senior Management becomes critical. The CAE must be close enough to the business to understand its strategy, priorities and challenges, while remaining sufficiently independent to challenge decisions and communicate



Chief Audit Officer

difficult messages objectively and courageously. This is the foundation of becoming a true Trusted Advisor. Management's reliance on Internal Audit for advisory services should result from the credibility and value demonstrated through its assurance work. Internal Audit can provide insight and advice, but must never assume management responsibility or compromise its independence. The strength of Internal Audit also depends on the institution's maturity level. A mature organization understands that Internal Audit is not simply a regulatory requirement or a box to be ticked. It is a strategic function requiring appropriate resources, authority, unrestricted access and continuous support from the Board and, particularly,

the Audit Committee.

In the banking sector, the Central Bank and regulatory authorities have an important role in continuously reinforcing this framework through requirements that support the independence, effectiveness and objectivity of Internal Audit, ultimately protecting depositors, shareholders, customers and other stakeholders.

Importantly, all of these dimensions should be reflected in Internal Audit scorecards and KPIs. Performance should not be driven predominantly by the number of audits completed or adherence to the annual plan. KPIs should also capture the quality and impact of assurance, risk coverage, timely escalation of significant and emerging risks, regulatory compliance, stakeholder confidence, and the sustainable value delivered to the institution—while preserving Internal Audit's independence. Ultimately, the question should not be: "Did Internal Audit complete its plan?"

The more important question is: "Did Internal Audit help the institution see what it could not see, anticipate emerging risks, and strengthen itself before risks become crises?"

A strong Internal Audit function is not simply an error-finding function. It is a function that protects trust, strengthens governance and contributes to the long-term sustainability of the institution.

Khaled Saeed's Words

From Governance on Paper to Governance in Practice

- A board can approve every policy, hold every scheduled meeting and still fail to govern well. The clearest warning sign is not a missing document. It is a room full of people who can explain the process, yet no one can say who owns the decision. Governance is tested when a difficult issue arises: who sees the full picture, who is willing to challenge, and who remains accountable after the meeting?
- One experience made this clear to me. A committee met on time and received good papers, yet members were largely being informed of decisions already made. There was little room to examine alternatives or question assumptions. What changed the meeting was practical: earlier papers, a clear statement of the decision required, and an honest record of dissent. Members finally had a real chance to influence the outcome.
- I saw a similar problem in a group with several entities. The line between matters reserved for the parent board and those delegated to subsidiary boards was unclear. Routine decisions travelled to the top,



while significant matters were handled locally. Everyone could point to an authority matrix, but no one could quickly explain who owned the decision. Clarifying reserved matters and escalation triggers improved speed and accountability. We did not need more approvals; we needed clearer ones.

- Conflict of interest is another area where the gap becomes obvious. The annual declaration matters, but the real test comes when an agenda item affects a board member, an executive or someone connected to them. Was the interest

disclosed? Did the individual step away? Did the minutes say so? Those details reveal more than the signed form.

- I have also seen sound board decisions lose momentum after a meeting. The discussion was recorded, but no one was named to act, no deadline was agreed, and there was no route for escalation. Follow-up is not housekeeping; it is part of governance. If the board cannot later see what happened to its decision, the process is incomplete.
- Internal Audit can give the board an independent view of whether these arrangements work, but it cannot govern on the board's behalf. My practical test is simple: six months later, can the organization explain a significant decision? It should be able to show what the board knew, what was challenged, who had authority and what happened next. For me, that is the difference between governance on paper and governance in practice.

Dina Moustafa's Words

Privacy Has a Deadline. Trust Doesn't.

"From 1 November 2026, Egypt's personal data protection framework enters a new phase of enforcement." A country of more than 117 million people and 96.3 million internet users is switching its data protection regime from paper to practice — and the switch has a date on it.[FE1.1] That is the day the grace period closes on the Executive Regulations to Personal Data Protection Law No. 151 of 2020[FE2.1], issued in November 2025 [FE3.1]after a five-year wait[FE4.1]. Overnight, privacy in Egypt moved from principle to permission. Most controllers and processors now need a license from the Personal Data Protection Centre. Cross-border transfers, electronic marketing and public surveillance each need their own. A breach buys you 72 hours to tell the regulator [FE5.1]and three working days to tell the people affected. Here is the uncomfortable truth: you cannot license what you cannot locate. Every organization I speak to is discovering the same thing — the hard part was never the legal text, it was knowing exactly what data you hold, why you hold it, and when it should have been deleted.

GRC Egypt Magazine



Data Protection Officer,
Vodafone Egypt

At Vodafone Egypt, we did not wait for the deadline to find out. We sat with the regulator over a year of working sessions and contributed to the drafting of the law itself, because we believe good regulation is built with industry, not at it. We have strengthened our assessment of high-risk suppliers through end-to-end, on-the-ground reviews rather than relying solely on questionnaires. We embedded privacy impact assessments into how projects are born rather than how they are approved. That work was recognized with a Vodafone Group Compliance and Privacy award, but the

real reward is simpler: when the Centre asks, we can answer.

The next test is already here. Egypt published its National AI Governance Framework [FE6.1] in March 2026, with a tiered, risk-based model sitting alongside the Charter for Responsible AI and the National AI Strategy 2025–2030. A binding AI law is still in draft, and I hear the same reflex everywhere: we will govern AI when the law arrives.

It already has. Wherever a model touches personal data, the PDPL governs it today. Purpose limitation, lawful basis, transparency and data subject rights bind an algorithm exactly as they bind a database. Waiting for AI-specific legislation is not caution — it is exposure. So my message to fellow practitioners is this. Stop treating November as a finish line. Licensing readiness is not a project; it is an operating model. Privacy is not the signature at the end of the slide deck; it is the question asked before anyone builds anything.

Regulators will keep writing rules. Customers only ever read one thing: whether we deserved their data.

Dr. Hanan Amin's Words

Resilience Without Walls: The Economic Case for Unified Governance in an Era of Trade Fragmentation

Global Trade in 2026 is neither collapsing nor thriving. The World Trade Organization (WTO)'s Report 2026 estimates that in a geo-fragmented world, global GDP would fall by 5.1 percent and exports by 18.6 percent, with smaller and poorer economies losing more than three times as much as high-income countries. Yet fragmentation remains the accumulated results of policy choices that can be reversed.

The numbers behind the anxiety are real. In the first ten months in 2025, over 2,500 trade restrictions were imposed worldwide, almost five times the 2015 level, and trade policy uncertainty has averaged nearly five times its 2000s level. Tariffs rose in 2025, manufacturing hit hardest, and two-thirds of global trade now runs through value chains being reshaped by geopolitics, industrial policy, and new technology. Firms are diversifying suppliers and relocating production closer to key markets, the result is a "Re-globalization" in which trade stays dense between countries that trust each other, and much thinner between rivals.

From an economic standpoint, diversification carries a cost today, but it pays for itself when disruption strikes. IMF modelling confirms this logic. For goods heavily sourced from a single bloc, diversifying suppliers cuts

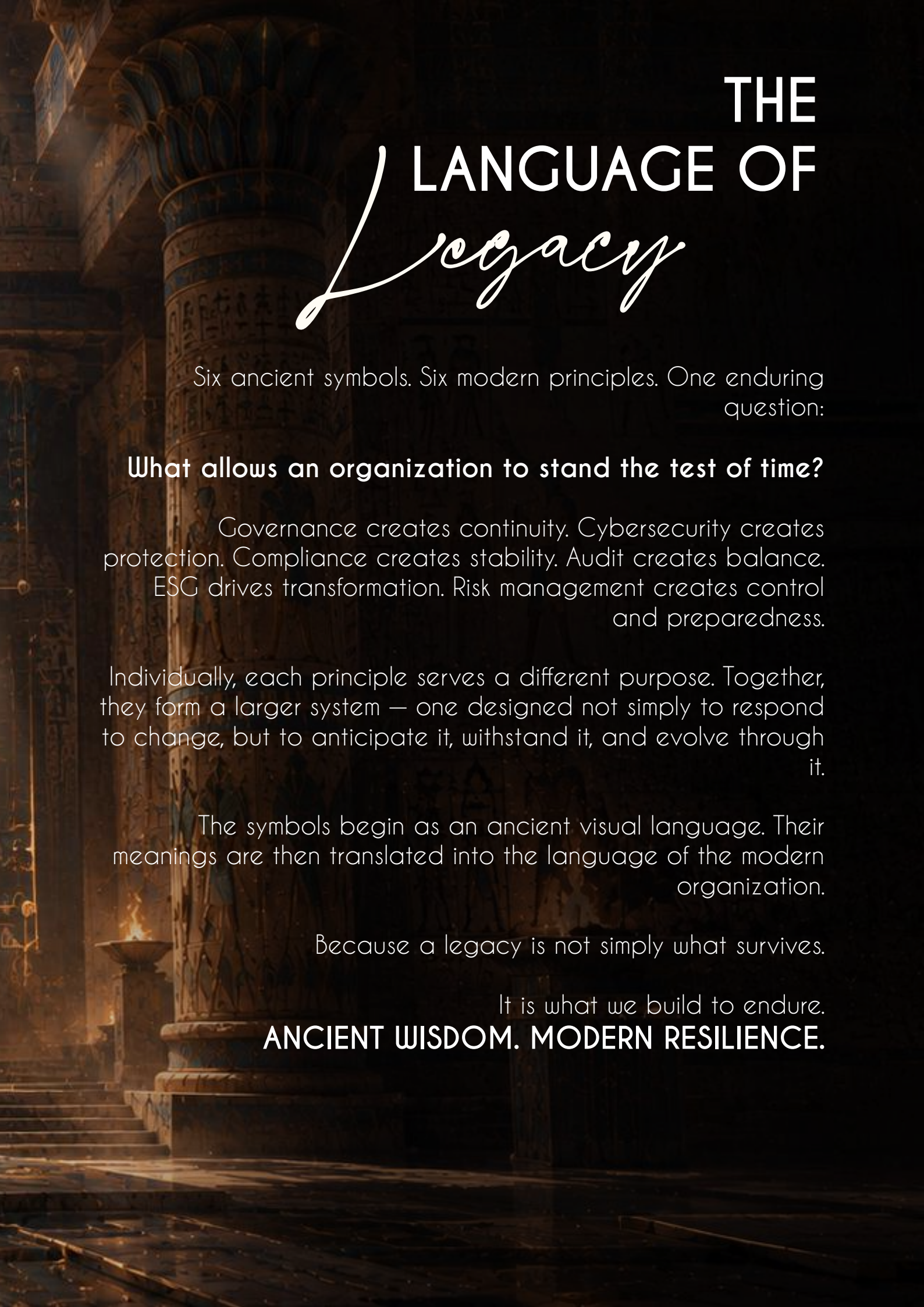


welfare losses by 12 percent if fragmentation actually occurs, and the insurance is worthwhile even if the chance of that scenario is only 7 to 9 percent. In other words, prudence, not protectionism, can justify some redundancy. But redundancy works best when it is shared. If every country builds its own duplicate stockpiles and supply lines, the costs multiply while the protection barely improves; when countries pool stockpiles, align standards and make their rules interoperable, the same resilience costs each of them far less.

Yet resilience that stops at national borders has its limits. Export controls, screening regimes and rival technical standards behave like broad

non-tariff barriers that raise costs for everyone, including the countries that impose them. This is the contradiction of fragmented resilience. Each country's attempt at self-protection raises costs and severs trade links for everyone, so the whole system, including the countries that built the walls, becomes more fragile. Meanwhile the WTO's dispute-settlement system remains paralyzed, leaving smaller economies exposed to unilateral coercion they cannot resist. Restoring binding dispute settlements, updating rules for digital and green trade, and coordinating resilience instruments across borders would let economies insure against shocks without paying the fragmentation tax twice. Promisingly, cooperation is quietly rebuilding through bilateral and regional channels. More than a dozen trade agreements were signed this year, roughly double the 2020-2024 pace, as governments seek diversified partners and regional supply chains. Yet the broader lesson remains, open and diversified trade is the most powerful resilience technology humanity has devised, while walls are a costly substitute. The task of 2026 is not to choose between efficiency and security, but to build the shared governance that delivers both.



The background of the entire slide is a photograph of an ancient Egyptian temple interior. It features large, ornate columns with hieroglyphs and papyrus capitals. The lighting is dramatic, with warm, golden light filtering through the columns, creating a sense of depth and history. The floor is made of large stone tiles, and the overall atmosphere is one of ancient grandeur and mystery.

THE LANGUAGE OF *Legacy*

Six ancient symbols. Six modern principles. One enduring question:

What allows an organization to stand the test of time?

Governance creates continuity. Cybersecurity creates protection. Compliance creates stability. Audit creates balance. ESG drives transformation. Risk management creates control and preparedness.

Individually, each principle serves a different purpose. Together, they form a larger system — one designed not simply to respond to change, but to anticipate it, withstand it, and evolve through it.

The symbols begin as an ancient visual language. Their meanings are then translated into the language of the modern organization.

Because a legacy is not simply what survives.

It is what we build to endure.

ANCIENT WISDOM. MODERN RESILIENCE.

LEGACY FORWARD

Like the enduring symbols of Ancient Egypt, true governance, resilience, and sustainability are built not only for today, but for the generations that follow.

GRC Summit Egypt

For advertising, printing, & further information, contact us on

mag@grcsummiteg.com

[For Subscription Click Here](#)

www.grcsummiteg.com

[in](#) [grcsummit.eg](#) [ig](#) [grcsummit.eg](#) [f](#) [grcsummit.eg](#)
[grcsummiteg](#)

©2026 FIG Solutions and GRC Summit Egypt.
All rights reserved.