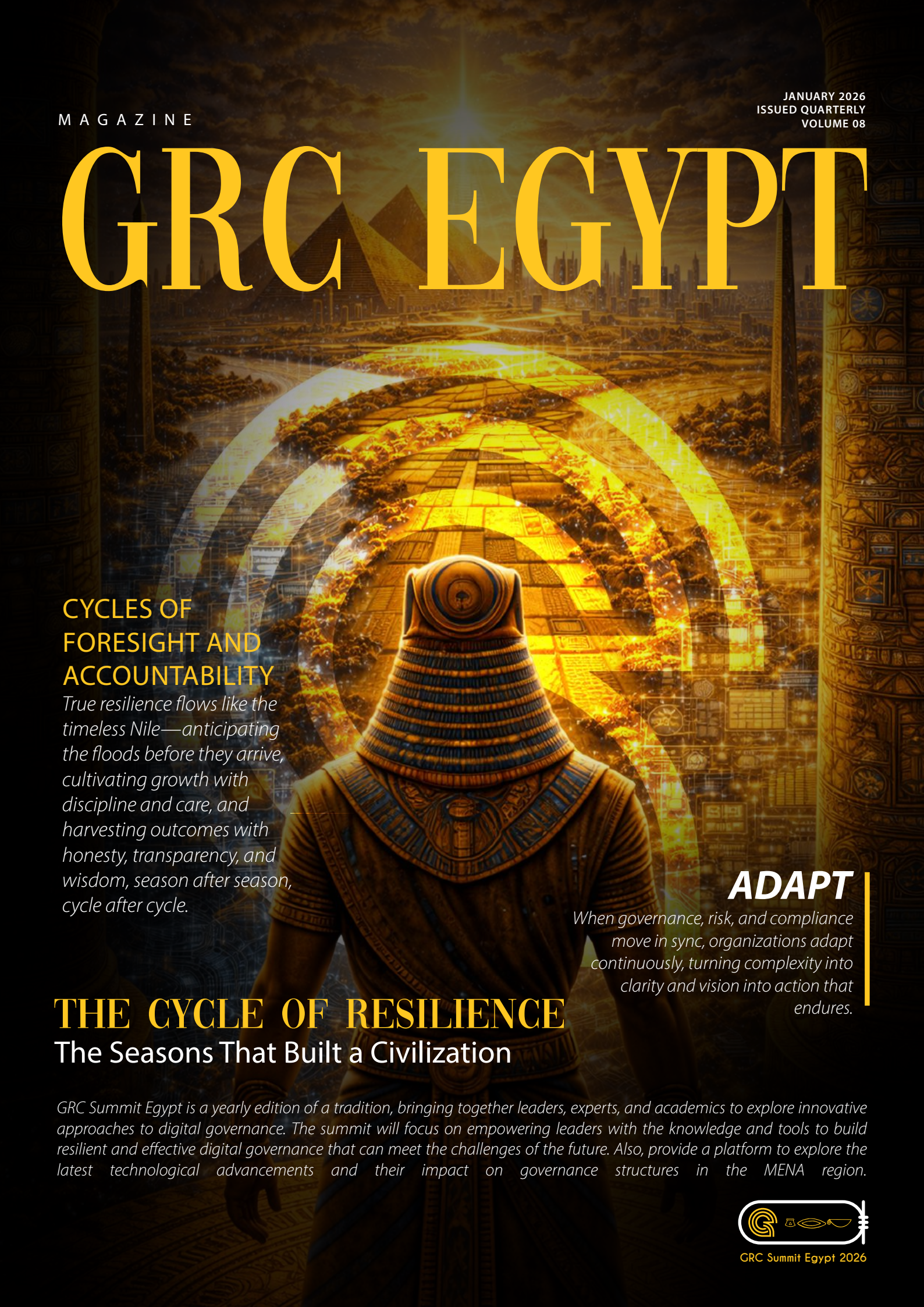
MAGAZINE

JANUARY 2026
ISSUED QUARTERLY
VOLUME 08

GRC EGYPT



CYCLES OF FORESIGHT AND ACCOUNTABILITY

True resilience flows like the timeless Nile—anticipating the floods before they arrive, cultivating growth with discipline and care, and harvesting outcomes with honesty, transparency, and wisdom, season after season, cycle after cycle.

ADAPT

When governance, risk, and compliance move in sync, organizations adapt continuously, turning complexity into clarity and vision into action that endures.

THE CYCLE OF RESILIENCE

The Seasons That Built a Civilization

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.

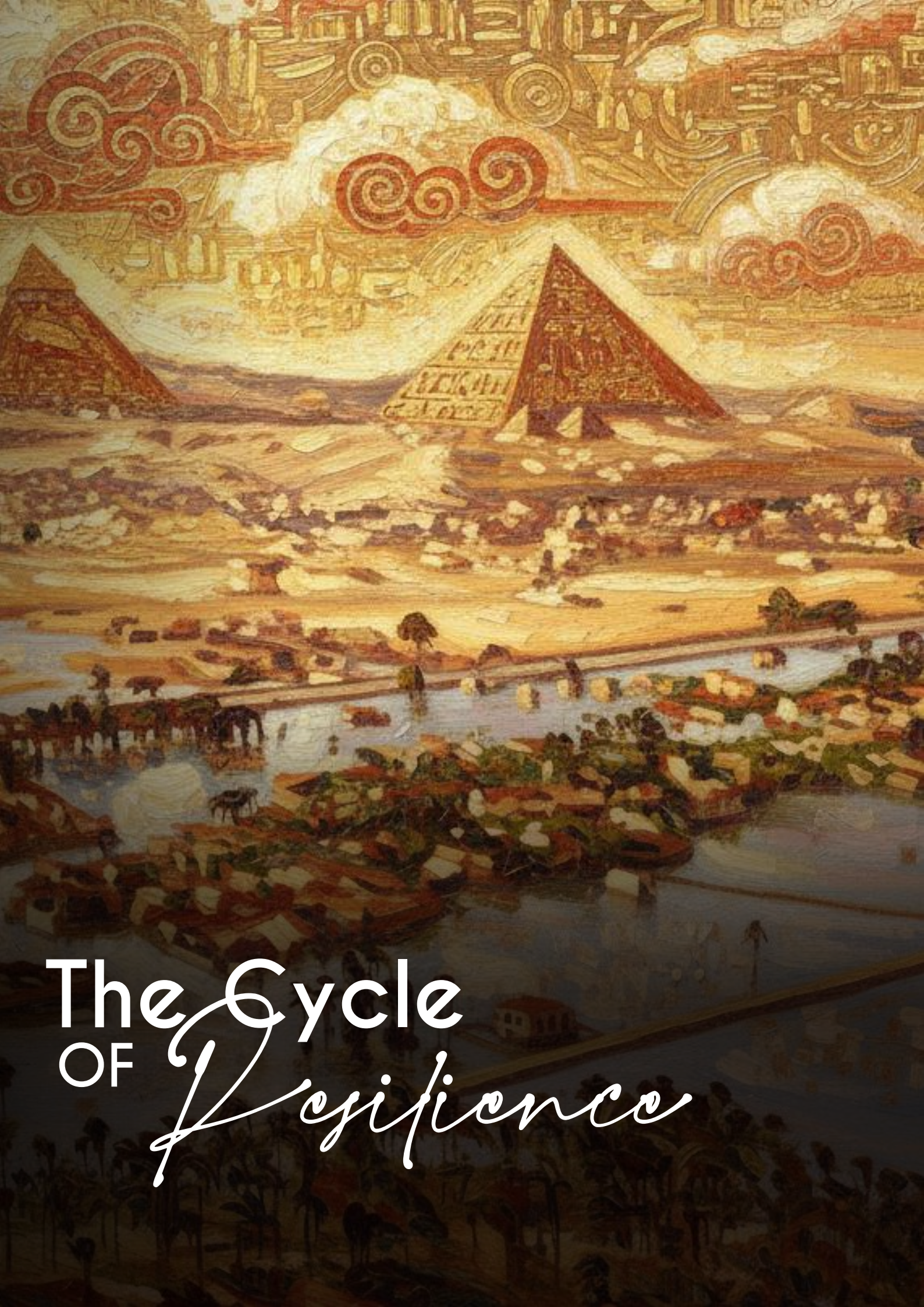
GRC Summit Egypt 2026

The Seasons That Built a Civilization

Long before the modern world defined its quarters, reporting cycles, or strategic planning frameworks, Ancient Egypt organized its entire society around a simple, elegant rhythm: three seasons shaped by the Nile. Akhet, Peret, and Shemu were more than agricultural phases—they were a national operating system. They dictated food production, religious ceremonies, taxation, labor, governance, infrastructure, and even national stability. Every citizen, from farmer to pharaoh, lived in sync with these natural cycles.

The annual flooding, the gradual emergence of fertile land, and the final harvest formed a predictable pattern that sustained one of history's most enduring civilizations for over 3,000 years. These seasons taught the Egyptians to prepare before crisis, act with structure during growth, and evaluate results with clarity.

In this issue, we revisit these ancient rhythms not as relics of history, but as timeless strategic models. Today's organizations face different challenges—cyber threats, regulatory pressure, climate expectations, operational risk—but the logic of cyclical resilience remains the same. By examining how the Egyptians navigated change, prepared for uncertainty, and built systematic stability, we uncover a framework that speaks powerfully to modern governance, risk, compliance, ESG, cybersecurity, and audit practices.


The Cycle
OF
Decidence

Dr. Lamise A. Negm's Words

Vocational Education as National Engine: A Strategic Vision

Vocational education in Egypt is ready for transformation—an opportunity to establish it as a fully integrated component of the national development framework with enhanced resources and strategic positioning within the education ecosystem. In an era defined by rapid economic transformation, this sector represents a critical enabler of inclusive growth, social cohesion, and sustained competitiveness.

"Empowering vocational education is not an educational reform, it is a national investment in our youth, our productivity, and Egypt's future competitiveness."

Egypt stands at a pivotal juncture. Demographic opportunities, accelerating digital transformation, and evolving global economic dynamics call for a workforce characterized by technical proficiency, adaptability, and future readiness. Vocational and technical education is positioned to serve as a foundational pillar of national human capital development, complementing academic pathways to meet this imperative.

The potential impact extends across multiple dimensions of national development. A strengthened vocational system can address employment opportunities for youth, support industrial advancement, and contribute to Egypt's vision of becoming a regional manufacturing and services hub.

Advancing vocational education requires comprehensive systemic enhancement. First, curricula can be strategically aligned with labor market opportunities, particularly within priority sectors including manufacturing, renewable energy, logistics, agribusiness, construction, and digital services. This alignment encompasses substantive collaboration with private sector stakeholders, industry associations, and international development partners, ensuring relevance, quality assurance, and enhanced employability outcomes.

Second, robust institutional governance provides the foundation for success. Effective frameworks with transparent accountability mechanisms and outcome-oriented performance indicators are essential. Impact can be measured through demonstrable metrics including graduate employment rates, wage progression, productivity enhancements, and contributions to economic value creation. This methodology reinforces Egypt's commitment to operational efficiency, institutional transparency, and evidence-informed policy development.

"A better future for Egypt's youth begins when education creates skills, dignity, and real pathways to economic participation."

Third, societal perception presents an opportunity for strategic evolution. Enhanced recognition follows from sustained investment in instructor professional development, modern training infrastructure, and clearly articulated career advancement pathways. When vocational trajectories lead to professional dignity, economic security, and entrepreneurial opportunity, broader social acceptance naturally strengthens, creating a cycle of enrollment growth, quality improvement, and economic contribution.

"When vocational education is strengthened, youth are empowered, industries advance, and the future of Egypt becomes sustainable by design."

ON PREMIERE SCREENING

STAY TUNED
GRCSEG26

FOUR SEASONS
SHARM EL-SHEIKH
04.02
2026

THIS FEBRUARY

www.grcsummiteg.com

THE KEMET SYMPHONY

In a world shaped by ancient forces and guided by timeless wisdom, Egypt rises once more—where the Nile first carved civilization, gods forged the earliest codes of order, and cinema rekindled the nation's voice. From sacred governance to modern digital resilience, from the blueprints of the ancients to the orchestration of a data-driven future, a legacy awakens. Across millennia of discipline, balance, vigilance, and truth, Egypt now stands at the threshold of a new era—summoning the world to witness a story still being written, a destiny still unfolding, and a future we will orchestrate together.

Alaa El Zoheiry's Words

At the Crossroads: MENA Insurance in 2026 Amid Geopolitics, Climate Stress, Cyber Threats, and Digital Disruption

Chairman of the Insurance Federation of Egypt & Managing Director of GIG Egypt

The Middle East has historically been a region prone to geopolitical tensions which can affect both underwriting profitability and risk exposure. Reinsurers may face increasing demand for coverage against political violence. What to Expect in 2026: A more complex risk environment where political risks continue to be significant. Insurers and reinsurers may need to reassess their portfolios and pricing structures, particularly for high-risk countries.

While the Middle East may not face as many natural disasters as other regions, climate change is contributing to rising temperatures, water scarcity, and extreme weather events. As a result, there will likely be an uptick in the need for property and agriculture insurance, and for more sophisticated risk models to address these emerging threats.

A growing demand for climate risk coverage, especially in countries like Egypt, which is highly vulnerable to the effects of climate change, such as rising sea levels and desertification.

As digital transformation accelerates, cyber threats are becoming an increasing concern for insurers, reinsurers, and their clients. Data breaches, ransomware attacks, and other forms of cybercrime will be on the rise, requiring more sophisticated risk management strategies. Cyber risk will emerge as a key area for insurers to focus on. There will be an increased push for cyber insurance products, and insurers will need to partner with cybersecurity experts to mitigate risks

Economic instability, currency fluctuations, and inflation are persistent risks in many parts of the Middle East and North Africa (MENA). Regulatory frameworks are also evolving, with increased scrutiny from governments and regulators over solvency and capital requirements. Rising regulatory pressures around solvency margins, liquidity, and consumer protection. Additionally, economic volatility could lead to higher claims ratios and financial instability in certain market

Strategic Priorities for 2026

The region has seen an increase in digital adoption, and insurers must continue to innovate in this space, offering online platforms, digital claims processing, and AI-powered underwriting. Increased focus on Insurtech, AI, and automation to enhance operational efficiency, improve customer experience, and streamline claims processing. Insurers and reinsurers will need to invest heavily in digital solutions to remain competitive.

Consumers in the Middle East and Egypt are increasingly looking for more personalized and comprehensive insurance products. There's a growing demand for products that cover emerging risks, such as cyber, climate change, and new health challenges. Expanding beyond traditional lines of insurance (e.g., life, health, auto, property) to cover new areas like cyber liability, climate risk, and economy-related insurance

products.

Investors, regulators, and consumers are increasingly prioritizing Environmental, Social, and Governance (ESG) factors. The insurance sector is under pressure to adopt sustainable business practices. More insurers will align with global sustainability goals, incorporating ESG criteria into their investment portfolios, underwriting processes, and product offerings. Reinsurers will need to consider ESG risks when developing their models, especially in relation to climate change

There are opportunities to expand into underserved markets within MENA, such as rural areas in Egypt or emerging economies like Iraq and Libya. The growing middle class and rising awareness of insurance in these markets present opportunities for insurers to increase penetration. Insurers may look to expand into high-growth markets within the region, particularly in countries with low insurance penetration. Partnerships with local players and the development of affordable micro-insurance products could be a strategy to tap into these markets.

Customers are becoming more demanding and expect personalized, seamless experiences across digital channels. Insurers will need to prioritize customer service, responsiveness, and flexibility in their offerings. Insurers will increasingly adopt a customer-centric approach, utilizing data analytics to tailor products and services. A focus on digital-first and omnichannel strategies will be key to attracting younger, tech-savvy consumers.
Possible Challenges

While the region is gradually embracing insurance, there are still cultural challenges around the perception of insurance as a product, particularly in countries with low penetration rates. Educating consumers about the benefits of insurance will remain a key hurdle.

Economic fluctuations, increased competition, and the challenges of underwriting emerging risks could result in pricing pressures. Insurers will need to strike a balance between offering competitive pricing and maintaining profitability.

As risks increase (e.g., from climate change, cyber threats), reinsurers may raise prices or reduce capacity, making reinsurance more expensive and harder to obtain for primary insurers. This could lead to increased costs for policyholders and potential coverage gaps.

With different countries in the region having varied regulations, insurers operating in multiple jurisdictions could face challenges navigating complex regulatory frameworks. The regulatory environment is evolving, and companies will need to stay agile to remain compl

Opportunities for 2026
Egypt, with its large population and growing middle class, represents a huge opportunity for insurers. The country's low insurance penetration rate offers significant upside for companies looking to expand their footprint in the region.
Opportunity in 2026:

Growth of insurance products in Egypt and other MENA countries with similar demographics could be a major focus. Micro-insurance and affordable health insurance options will be key areas of development.

Collaboration between traditional insurers and Insurtech startups will become increasingly important to drive innovation and efficiency. Insurers that partner with Insurtech's to offer digital-first solutions and improve underwriting and claims processing will gain a competitive edge.

With the growing focus on healthcare, wellness, and preventive care, insurers can tap into new markets by offering products that focus not just on healthcare but also on promoting wellness. The rise of personalized health insurance, combining coverage with wellness programs (e.g., fitness tracking, preventative health), could see greater uptake in the region

Given the increasing focus on climate change, insurers could innovate with products specifically designed to help businesses and individuals adapt to and mitigate the impact of climate risks. Climate resilience insurance could become a key product line, especially for sectors like agriculture, real estate, and energy.

Dr. Ahmed Galal's Words

Dr. Ahmed Galal, CEO and Managing Director of EBank, emphasized that the shift towards algorithms and artificial intelligence in banking presents significant opportunities to enhance efficiency and accelerate decision-making, while underscoring the importance of keeping the human element at the core of the system. He explained that the Bank's strategy leverages technology as a supportive tool for humans to promote financial inclusion, in alignment with the Central Bank of Egypt's directives and Egypt's Vision 2030, during his participation in the GRC Egypt Summit.

He noted that effective governance extends beyond policies and procedures to encompass organizational mindset, highlighting that many risks stem from unintended human biases in decision-making. Dr. Galal emphasized the importance of cultivating a corporate culture that promotes objective discussion and diverse perspectives to enhance decision quality and mitigate risks. He also pointed out that expanding the use of data and digital services requires a careful balance between delivering real value to clients and protecting their privacy, alongside implementing smart monitoring systems for early risk detection and proactive response. He concluded by reaffirming that governance at EBank serves as a key instrument for building a resilient and sustainable banking institution that supports economic growth and Egypt's broader development objectives.

CEO and Managing Director – EBank

CEO & MD The united Bank

Tarek Fayed's Words

The Human Dividend: Why Autonomous Finance Still Needs Empathy

Banks are moving rapidly toward Autonomous Finance, where artificial intelligence makes lending and credit decisions in real time. The efficiency gains are evident: faster approvals, scalable risk assessment, and consistent outcomes. Yet a fundamental question is emerging at board and executive levels—what happens to trust when judgment becomes fully automated?

Lending has never been purely mathematical. Every credit decision carries social and economic consequences, particularly for SMEs, first-time borrowers, and underserved segments. AI models are trained on historical data, and history often contains bias, exclusion, and structural inequality. Without deliberate governance, algorithms do not eliminate these issues; instead, they can unintentionally amplify and institutionalize them at scale.

This is where the concept of the Human Dividend becomes critical. The Human Dividend represents the incremental value created when human judgment, empathy, and accountability are intentionally embedded within AI-driven decision-making. It is not a rejection of automation, but an acknowledgment that responsible banking requires more than statistical accuracy and model performance.

Traditional Governance, Risk, and Compliance frameworks were designed for humans making decisions. In an era of black-box algorithms, GRC must evolve from a control function into a guardian of ethical autonomy. Boards should mandate Human-in-the-Loop governance, ensuring that high-impact credit decisions remain explainable, challengeable, and ultimately accountable to people, not systems.

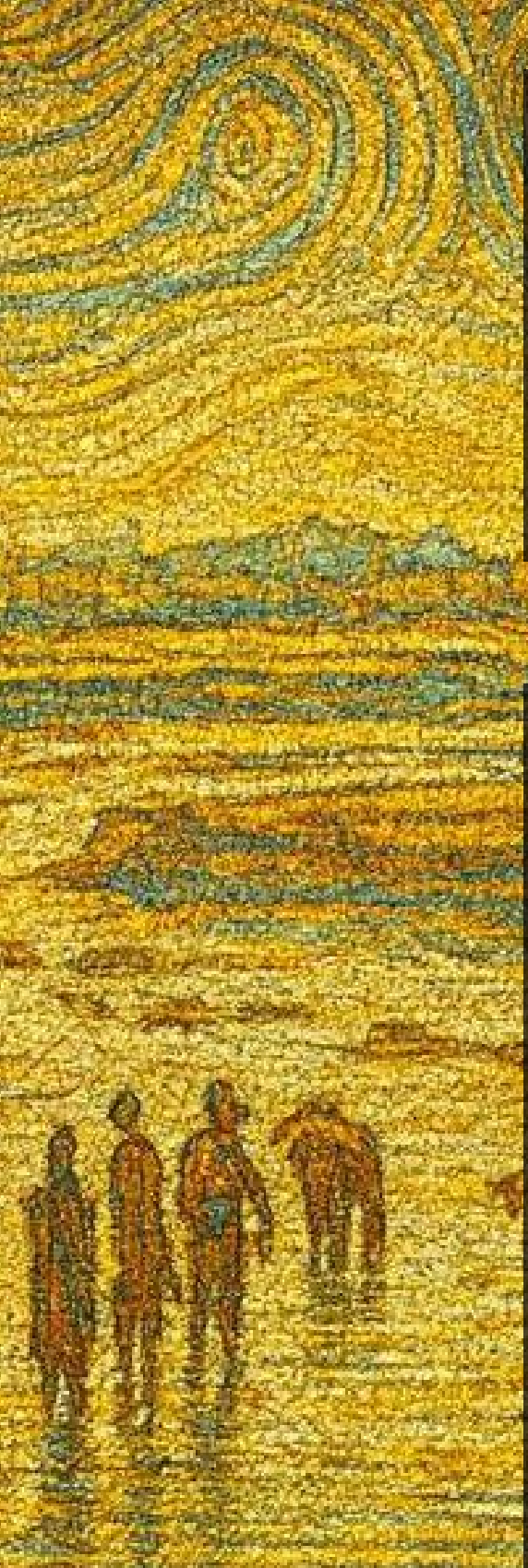
This approach reflects the Ethics of Empathy. Empathy does not weaken credit discipline; it strengthens trust and sustainability. It can be governed through explainability standards, bias monitoring, escalation thresholds, and inclusion metrics treated as material non-financial risks.

In the age of Autonomous Finance, competitive advantage will not be defined by who has the most advanced algorithm, but by who governs intelligence with humanity. The banks that preserve the Human Dividend will be the ones that earn lasting trust.

Akhet

— The Flood of Governance

(Inundation / Foundation Season: Mid-July to Mid-November)

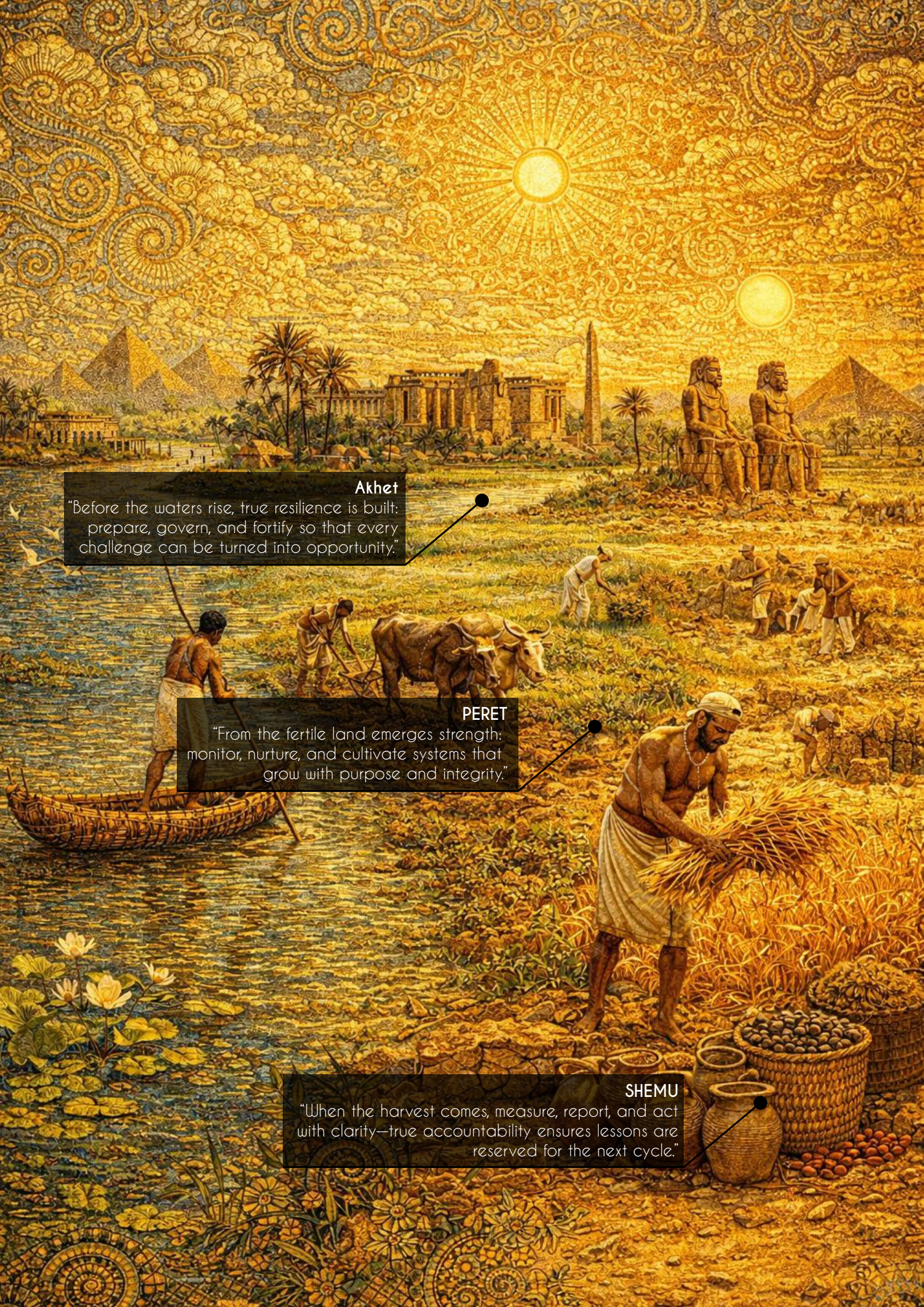


Akhet marked the dramatic rise of the Nile, when its waters flooded the fields and transformed the landscape into a vast, shimmering expanse. This was a time of renewal and anticipation, as the floodwaters deposited rich, dark silt that made agriculture possible. The season represented the power of divine order, with Hapi—god of the Nile's bounty—honored for sustaining life. During Akhet, no planting occurred; instead, people repaired canals, recorded flood levels, and prepared for the agricultural year ahead. Its months—Thoth, Phaophi, Athyr, and Khoiak—aligned with major religious celebrations, reinforcing the belief that cosmic balance and earthly prosperity were deeply intertwined.

Meaning: The Nile floods covered the land, depositing fertile silt — the start of the agricultural year.

Deity: Hapi, God of the Nile Flood

Symbolism: Renewal, cleansing, and foundation.


Akhet
"Before the waters rise, true resilience is built: prepare, govern, and fortify so that every challenge can be turned into opportunity."
PERET
"From the fertile land emerges strength: monitor, nurture, and cultivate systems that grow with purpose and integrity."
SHEMU
"When the harvest comes, measure, report, and act with clarity—true accountability ensures lessons are reserved for the next cycle."

Akef El Maghraby's Words

AI Is the New Era of Banking: Innovation with Guardrails


Chief Executive Officer & Managing Director of Suez Canal Bank

For leaders in the financial sector, digital transformation has been the key differentiator over the past two decades. What began as a basic IT support function has evolved into advanced digital capabilities that drive business value, from enabling digital channels to reaching remote customers and generating revenue through superior journeys and experiences in a competitive environment. The financial landscape is now dominated by digital progress, with government policies such as cashless-economy initiatives and the launch of digital products shifting the industry's focus.

We are discovering now that all of this was a pre-stage preparation for the new era. AI is the new era, whether for companies building AI or utilizing it. AI has become the new language that is transforming all aspects of life. As the industrial revolution ushered in a new era, AI is doing the same now; it's closing gaps and creating new ones, creating opportunities, and reshaping human life everywhere.
AI offers transformative opportunities in all fields. In the financial sector, use cases include fraud detection, credit scoring, operational efficiency, and customer experience. For businesses, the question now is not whether to adopt AI, but how to do it responsibly.

Personally, I believe AI will reshape the financial sector in the coming years, and, as always, early adopters are the risk-takers and the harvesters of greater value realization. With AI no longer seen as a choice, the roles of Governance, Risk, and Compliance (GRC) and Cybersecurity have become more critical for the adoption and use of this new field. Artificial Intelligence (AI) is reshaping the global financial landscape, introducing unprecedented opportunities for efficiency, personalization, and growth. Yet it also introduces new dimensions of risk, cybersecurity threats, and ethical, operational, and regulatory aspects that demand proactive strategies. Guardrails became the most mandatory initial step to build, operate, and enable a sustained AI adoption.

In the Global Cybersecurity Outlook 2025 published by the World Economic Forum WEF, it emphasizes the complexity in cybersecurity due to multiple factors and intense complexity and interlinking factors such as AI and emerging tech, regulatory requirements, supply chain interdependencies, and other factors. This complexity requires robust, brave, and context-aware GRC and cybersecurity programs that can harvest the gains and be risk-aware.

Boards and shareholders are looking to maximize the value of their businesses, and the trend of investing in the AI field is creating many opportunities that require intentional choices while pushing governance, cybersecurity, and assurance functions to take on their roles with clear responsibilities from day zero.

At Suez Canal Bank, we see AI as a central enabler of our strategy. Our transformation journey is laser-focused: integrate advanced technologies while upholding the highest standards of governance and cybersecurity. This ensures innovation is not decoupled from trust, redefining the future of banking.

Ramsés Gallego's Words

The RISK equation and additional taxonomy

Risk in inherent in life. Every organization in the world knows that with any business activity there is risk to identify and manage. And our customers would appreciate a vendor, a partner that fully understands the risk equation: a THREAT that exploits a VULNERABILITY, with a PROBABILITY of that happening and with an IMPACT.

These four variables make the risk equation and it is great for a conversation about understanding the society we live in and the exposure of companies around the planet. But interestingly enough, one can only work on three of those four variables. While we cannot avoid that THREATS exist (we may through a better and equal society, better education, etc. but this is not the topic of this message), we can heavily work on understanding VULNERABILITIES, reducing the PROBABILITY and mitigating the IMPACT.

A robust and sound cybersecurity strategy must work towards comprehending the assets that an entity has and which vulnerabilities exist on that universe of devices, infrastructure and platforms. Vulnerabilities take the form of a faulty code, a misconfiguration with identities or an unpatched server or endpoint that may mean the entrance for cyberattackers to bring the company at a halt. Consequently, vulnerabilty management through the

Chief Technologist, Cybersecurity, DXC Technology, ISACA Hall of Fame and IFGICT Fellow

insights that Identity and Access Management and Application Security bring -to name just two- are fundamental to success. In an nutshell, there might exist a threat... but if there is no vulnerability -a hole in your wall-, there's little for that threat to do.

Reducing the probability of all that is also imperative for a risk mitigation strategy to shine. And a company can do that by leveraging technology within the field of Security Operations and Application Security to understand changes in the environment, the security posture compared to a week or month before, etc. Giving less chance to attackers is fundamental to protect and defend what matters most: people and data.

Last, but not least, ensuring that if it happens, the impact is minimal -or even zero- is also a great part of a cybersecurity strategy: as an example, having the information protected with encryption and tokenization, having techniques for information not being useful out of a 'circle of trust' is critical in this scenario. Through the enforcement of processes and procedures that discover, identify and protect data in the area of Data Privacy and Protection an organization can reduce the impact (making the information useless) if, unfortunately, it is breached.

In short, the simplest risk equation is made out of THREATS - VULNERABILITIES - PROBABILITY - IMPACT and the flow that it goes with it. And it is fantastic for conversation with customers around the many angles that they mean in the dimensions of IDENTITIES - DATA - APPLICATIONS.

Additional taxonomy in this space are VaR (Value at Risk): understanding what's at stake, comprehending the value of our assets and what we need to protect... in order to defend with the appropriate countermeasures. The VaR exercise is great to have a profound view of the appreciation for information and data at large. It should not be forgotten that this all brings the concept of EF (Exposure Factor). There are companies that are more exposed than others, organizations with devices connected to the information highway in a deeper way and that deserves an assessment and comprehension so as to decide and define the right mitigation strategies.

Risk is inherent in life. So is Protection and Defense.

Sherif Elbehery's Words

Launching onebank, Egypt's First Digital Bank: From Vision to Execution


Chief Executive Officer, onebank

The question facing the banking industry today is no longer whether digital transformation is necessary, but how banks can fundamentally redefine their role in customers' lives. Over the past decade, customer expectations have evolved rapidly. Speed, accessibility, personalization, and seamless user experience are no longer differentiators, but baseline expectations. Customers now benchmark banks against the best digital experiences across retail, transportation, media, and entertainment. In this environment, incremental digitization of traditional banking models is insufficient; what is required is a deeper rethinking of how banks are built, operate, and are experienced.

This belief drove the launch of onebank, Egypt's first digital bank. onebank was not created as a digital layer on top of a conventional institution, nor as a mobile interface for existing products. It was built from the ground up as a fully digital bank, based on the idea that banking should integrate naturally into customers' daily lives, eliminating unnecessary complexity and friction. The ambition was to move beyond digital products toward a complete and evolving digital banking ecosystem.

Globally, fintech-driven disruption has reshaped customer expectations. People no longer compare banks only to other banks, but to the most intuitive digital platforms available. In Egypt, this shift is particularly pronounced. A young, digitally savvy population, high mobile penetration, and a strong focus on financial inclusion have increased demand for banking models aligned with immediacy, clarity, and convenience. For many customers, traditional branch-based banking feels increasingly disconnected from daily reality.

At the same time, Egypt's banking sector operates within a robust regulatory framework that balances innovation with stability and consumer protection. The Central Bank of Egypt has played a pivotal role in enabling responsible innovation, creating conditions for new digital banking models to emerge with confidence and strong governance.

From the outset, building onebank required a fundamentally different mindset than transforming an existing institution. Instead of automating legacy processes, the bank was designed by reimagining the entire value chain, starting with the customer journey. The vision was anchored in customer-centricity, digital-first design, and flexibility to evolve without legacy constraints.

Governance, risk, and compliance were embedded as core design principles rather than afterthoughts. Security, regulatory compliance, and risk frameworks were integrated from the earliest stages, supported by automation, real-time monitoring, and advanced analytics. Cybersecurity and data protection were positioned as trust enablers, not barriers to innovation.

The launch of onebank will reinforce a central lesson: availing such a digital proposition is not a one-time initiative, but an ongoing journey. Technology alone does not create differentiation; real value comes from combining innovation with strong governance, deep customer understanding, and strategic clarity. Banks of the next era are those that will balance agility with discipline, innovation with trust, and growth with resilience.

Chief Information Security & Risk Officer – Educational Board

Wessam Maher's Words

Long-Awaited Bylaw Enforces Egypt's Data Protection Law (PDPL)

Egypt's long-awaited executive bylaw for the Personal Data Protection Law (PDPL) has finally been issued, marking the point at which Law No. 151 of 2020 becomes fully enforceable. On 1 November 2025, the Minister of Communications and Information Technology published Executive Regulation No. 816 of 2025. It later appeared in the Official Gazette, ending five years of uncertainty surrounding implementation. With this regulation in place, the PDPL moves from a principles-based law into an operational legal framework with defined obligations, controls, and enforcement mechanisms.

For governance, risk, and compliance professionals, this development represents a material shift. Organizations operating in Egypt or processing personal data of Egyptian individuals are now subject to explicit compliance obligations. The regulation contains forty-two articles addressing data subject rights, breach notification, cross-border data transfers, governance structures, and the role of Data Protection Officers. These provisions collectively establish a structured privacy regime aligned with international standards while reflecting local regulatory priorities.

The bylaw reinforces and clarifies data subjects' rights. Individuals are granted the right to access their personal data, request corrections, seek erasure under specific conditions, and object to or restrict certain processing activities. Organizations are required to establish documented procedures to handle such requests within defined timelines and to provide justified responses when requests are denied. These requirements formalize accountability and remove ambiguity that previously existed due to the absence of implementing rules.

Special protection is afforded to children's personal data. The regulation prohibits the processing of personal data of individuals under 15 without verified parental or legal guardian consent. This higher consent threshold imposes additional operational responsibilities on organizations that collect or process data from minors, particularly in digital services, educational platforms, and online applications. Age-verification mechanisms and parental authorization processes are now regulatory expectations rather than best practices.

Breach notification is another central pillar of the regulation. Data controllers must notify the Personal Data Protection Centre within 72 hours of becoming aware of a personal data breach. This notification must include details on the nature of the breach, the categories and volume of data affected, the number of impacted individuals, the likely consequences, and the corrective measures taken or planned. Where a breach poses a risk to individuals' rights or freedoms, affected data subjects must also be informed promptly and in clear language. Even when notification thresholds are not met, organizations are required to document all incidents internally, reinforcing auditability and continuous improvement.

Cross-border data transfers are subject to strict oversight. As a general rule, transferring personal data outside Egypt requires prior authorization from the Personal Data Protection Centre and informed consent from the data subject after disclosure of the associated risks. Organizations

relying on international hosting, cloud platforms, or group-wide processing arrangements must reassess data flows, contractual safeguards, and regulatory approvals to ensure compliance with the new framework.

The regulation also formalizes the role of the Data Protection Officer. Organizations must appoint a qualified DPO and register the appointment with the relevant authority. The DPO is responsible for monitoring compliance, advising on data protection obligations, promoting internal awareness, and serving as the primary point of contact for both regulators and data subjects. The role requires sufficient expertise, independence, and organizational authority to be effective, positioning the DPO as a key governance function rather than a nominal role.

A one-year compliance grace period applies from the date the executive regulation is issued. During this period, organizations are expected to conduct gap assessments, register personal data databases, appoint and empower DPOs, update policies and procedures, implement breach response mechanisms, and train staff. While the transition period provides necessary breathing space, it should not be interpreted as a delay option. The scope and depth of the obligations mean that early and structured action is essential.

From a GRC perspective, the issuance of Executive Regulation No. 816 of 2025 is a positive and necessary milestone. It aligns Egypt's data protection framework more closely with global practices, reduces long-standing regulatory uncertainty, and enhances trust in the digital economy. At the same time, it shifts responsibility firmly onto organizations to demonstrate compliance in practice, not only on paper. The effectiveness of the PDPL will ultimately depend on execution, leadership commitment, and the organization's ability to embed privacy and accountability into daily operations rather than treating compliance as a one-off exercise.

Peret

— The Growth of Risk and Resilience

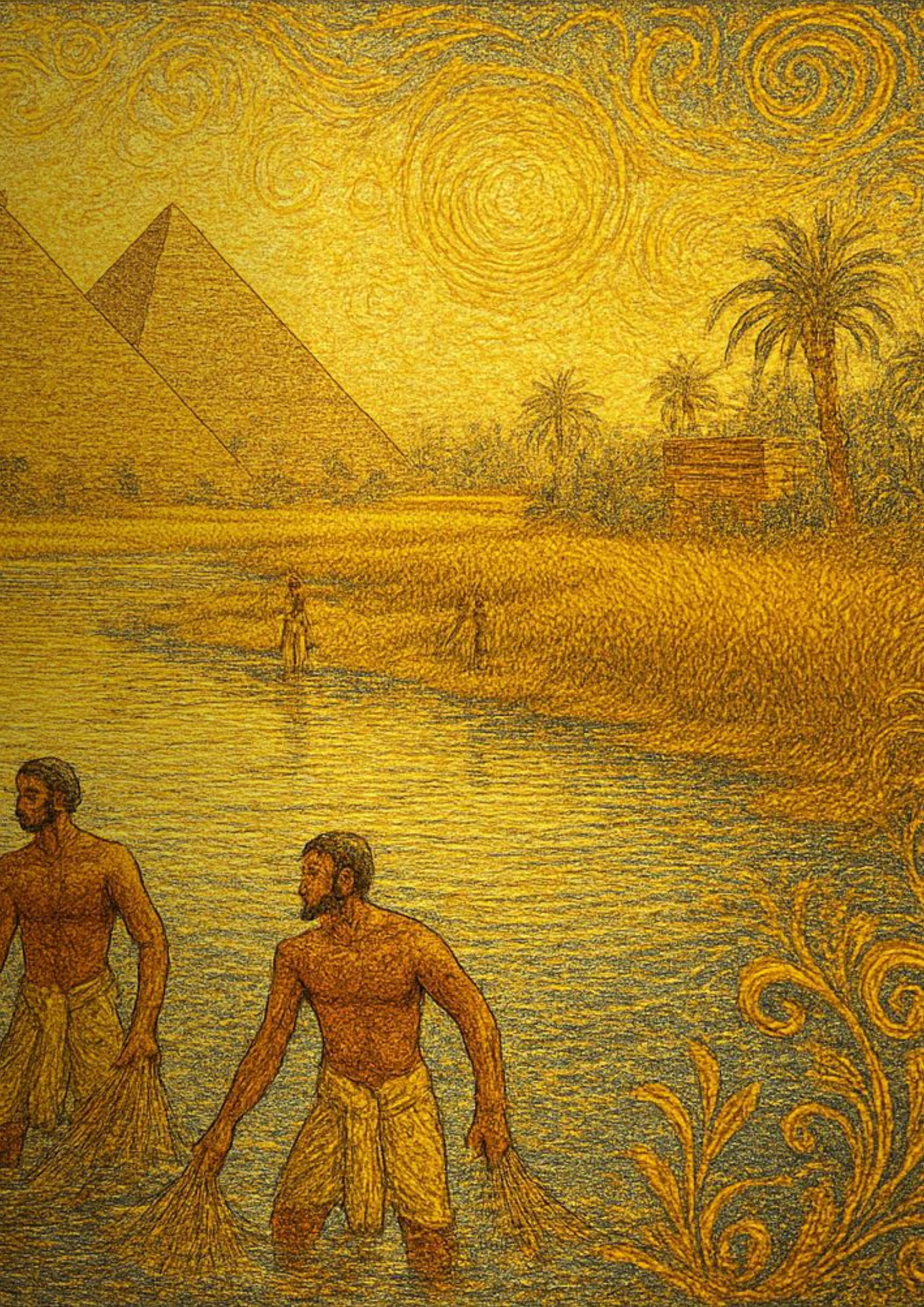
(Emergence / Growth Season: Mid-November to Mid-March)

Peret signaled the retreat of the floodwaters, revealing fertile land ready for cultivation. As the fields emerged from the flood, farmers plowed, sowed, and irrigated their crops, ushering in the most active agricultural phase of the year. This season symbolized rebirth and steady progress, mirrored by its patron deity Osiris, who embodied regeneration and the cycle of life. The months of Tybi, Mechir, Phamenoth, and Pharmuthi traced the crop's journey from planting to flourishing growth, supported by careful management of canals and water channels. Peret represented patience, diligence, and the promise of abundance—an essential bridge between nature's renewal and human effort.

Meaning: The land emerged from floodwaters, and crops began to grow.

Deity: Osiris, God of Rebirth and Vegetation

Symbolism: Growth, emergence, and resilience.



Dr. Komitas Stepanyan's Words

IT/Cybersecurity: Cost Center or Strategic Enabler?

This first article in a three-part series examines a common public-sector governance challenge: why executive teams often treat technology and cybersecurity as a cost center—and how GRC leaders can reframe them as strategic enablers of service continuity, resilience, and public trust.

Introduction

Public-sector organizations often underinvest in IT and cybersecurity—not because leaders "don't care," but because governance and measurement frequently fail to translate technical controls into outcomes that matter at the enterprise level. When reporting focuses on technical activity (patching, alerts, tool coverage) instead of mission impact (service availability, recovery time, citizen trust, regulatory exposure), cybersecurity naturally competes poorly for funding against visible frontline priorities.

This article explains why the cost-center mindset persists, how to express cyber value in executive terms, and what boards and executive committees can do to shift perception, accountability, and investment decisions.

Why the cost-center mindset persists

Boards and executive teams often view cybersecurity through a **compliance** or "insurance policy" lens rather than as **operational**

Technology & Cybersecurity Director, Central Bank of Armenia

resilience that protects service delivery and public confidence. Several patterns reinforce this:

- **Limited technology and cyber literacy at leadership level** leads to oversimplification ("we bought tools, therefore we're safe") or avoidance ("it's too technical").
- **Fragmented ownership and reporting lines** blur accountability across IT, risk, security, internal audit, and operations.
- **Misaligned KPIs** emphasize outputs (number of vulnerabilities closed, alerts handled, awareness sessions delivered) rather than outcomes (recovery time, service disruption exposure, critical process resilience).

This gap is directly addressed in **NIST CSF 2.0**, which elevates "**Govern**" as a core function to anchor cybersecurity in enterprise risk management, leadership decision-making, and accountability. Compared with earlier approaches that were often adopted as technical checklists, CSF 2.0 reinforces a clearer message: **cybersecurity governance is a leadership responsibility, not just an IT task.**

Quantifying strategic value in executive terms

To change perception, GRC leaders need to express cybersecurity as protection of **mission outcomes** and **financial exposure**, not as a growing list of technical requirements.

A practical approach is to combine business-aligned metrics with scenario modelling:

- Map priority incident types (ransomware, major outage, data integrity compromise, third-party failure) to:
  - **MTTR (Mean Time to Recovery)** and realistic recovery constraints
  - **Service impact** (affected citizen services, patient care, financial operations, utilities, etc.)
  - **Operational and financial exposure** (cost of downtime, overtime, backlog, reputational impact,

contractual/regulatory consequences)
This method reframes spending as investment in **recovery capability, continuity, and resilience**—with measurable reduction in disruption duration and downstream cost.

Regulatory and market drivers that force board attention

Oversight expectations are rising. Cybersecurity governance is increasingly treated as a board-level risk domain alongside finance, safety, and operational resilience. Newer requirements and guidance emphasize:

- **Leadership accountability and reporting expectations**
- **Timely incident notification and disclosure**
- **Demonstrable resilience and recovery readiness, not just preventive controls**

Adopting a governance-oriented approach aligned to **NIST CSF 2.0**, and strengthening management systems in line with **ISO/IEC 27001** and **ISO 22301**, helps leaders evidence due diligence, define ownership, and demonstrate readiness under scrutiny.

Practical board-level actions

Boards and executive committees **don't need to become technical experts**—but **they must enforce clear governance and accountability**. Practical steps include:

- **Translate cyber risk into mission and service metrics**

Board dashboards should include MTTR targets, service disruption exposure, recovery readiness, and critical process dependencies—not just tool activity.

- **Establish a "Govern" cadence**

Formalize executive oversight through recurring briefings, clear RASCI (or equivalent) accountability, and scenario-based exercises aligned to strategic objectives.

- **Use assurance mechanisms to validate investment decisions**

Leverage independent audits, third-party assurance, and (where used) insurance underwriting expectations to validate priorities and demonstrate reduction in exposure.

- **Prioritize continuous testing and recovery drills**

Shift the narrative from "prevention-only" to "assumed breach and recover fast." Treat recovery capability as a measurable operational requirement with regular exercises and lessons learned.

Conclusion

Reframing IT and cybersecurity as strategic enablers requires three things: evidence, governance, and accountability. When leaders see financially and operationally grounded metrics—and when governance structures align with the intent of NIST CSF 2.0's Govern function and management system standards like ISO/IEC 27001 and ISO 22301—cybersecurity stops being "an IT cost" and becomes what it is: protection of essential services, resilience, and public trust.

Mahmoud Elbagoury's Words

Internal Audit Vision 2035: From Assurance to Strategic Foresight

Internal Audit is entering a defining decade. By 2035, the profession will be reshaped by accelerating digital transformation, emerging risks, and heightened expectations from boards and regulators. The Internal Audit Foundation's Internal Audit: Vision 2035 – Creating Our Future Together sends a clear message: Internal Audit must evolve now to remain relevant and influential.

Chief Audit Executive (CAE), and Non-Executive Director (NED)

By 2035, Internal Audit will not be judged by how well it reports the past, but by how effectively it helps organizations navigate the future.

The traditional model of retrospective assurance is no longer sufficient in a world of real-time risk, artificial intelligence, and interconnected digital ecosystems. Vision 2035 reimagines the Internal Auditor as a strategic advisor; one who delivers not only assurance, but insight and foresight that enable organizations to anticipate disruption and protect long-term value.

Technology will be the primary catalyst of this transformation. Advanced analytics, continuous auditing, and AI-driven risk intelligence will redefine how assurance is delivered. Yet the real challenge is not technology itself, but mindset. Internal Audit must move from periodic review to continuous relevance, from control verification to strategic guidance.

Equally critical is the evolution of talent.
The Internal Auditor of 2035 must combine independence with curiosity, objectivity with business acumen, and technical competence with strategic vision. Multidisciplinary skills, adaptability, and learning agility will define professional credibility.

Vision 2035 is ultimately a call to leadership. Internal Audit's enterprise-wide perspective uniquely positions it to serve as an anchor of trust in uncertain times. By embracing intelligent assurance and strategic foresight, the profession can help organizations navigate complexity with confidence.

Amr El Gueziry's Words

GRC the idea and concept

With economic growth and rapid technological advancements, amidst regional and international challenges influenced by economic, political, and financial conditions, the financial and banking system is exposed to numerous risks that can impact the objectives and operations of financial and banking

CEO Consultant for GRC

institutions. Central banks and financial regulatory bodies play a vital role in establishing the rules and standards that monitor and protect financial institutions, as well as guiding and supporting them when needed.

Banks have in their structures control systems, some of which are mandatory according to regulations, and others which are optional according to the nature and size of the financial institution's business. These control systems have been defined as "lines of defense," where each line of defense undertakes specific tasks that are integrated in their entirety with the aim of identifying the risks facing the institution and analyzing them to reach their causes and whether there are gaps in the systems and executive tools that open the way for the emergence of those risks, and finally the impact of these risks on the financial institution's strategy and objectives, and proposing the necessary solutions to close those gaps and avoid their reappearance.

In practice, it was observed that each component of the control systems performed its role according to its work plan, while coordination between the components of the systems was lacking, which led to overlap in tasks and sometimes even conflict, and thus the impact decreased, and the benefit from the effort exerted in this important aspect decreased as well. Hence the need arose for an entity within banks to act as coordinator and organizer of defense lines at their various levels – a "maestro".

The GRC will act as the supervisory maestro for the financial institution, studying the components of the supervisory system, defining its roles and practices, and organizing the relationship between its parties to achieve the maximum possible benefit from the outputs of this system, which will contribute to giving a clear, honest, and unbiased picture of the risks that the institution faces or may face, enabling the business lines to put in place controls to avoid those risks.

It is worth noting that the central bank has established clear governance rules that can be considered fundamental pillars in building the GRC. The main objective of the GRC is to consolidate a risk matrix that reflects the level of risks an institution may face and its ability to withstand those risks.

Shemu

— The Harvest of Assurance and Sustainability

(Emergence / Growth Season: Mid-November to Mid-March)

Shemu was the culmination of the agricultural cycle—the season of harvest, gathering, and gratitude. Under the intense, drying heat of Ra, the sun god, crops ripened and workers moved quickly to collect grain before the fields turned arid. This was a time of productivity and celebration, as communities reaped the rewards of months of labor. The season's months—Pachons, Payni, Epiphi, and Mesore—were filled with festivals, offerings, and preparations for the upcoming new year. Shemu emphasized stewardship, foresight, and resilience, ensuring that granaries were full and society was ready for the coming inundation. Through this cycle, the Egyptians saw harmony between nature, divine will, and human responsibility.

Meaning: Harvesting crops and preparing for the next flood

Deity: Ra, God of the Sun

Symbolism: Illumination, evaluation, and renewal.

Dr. Mohamed El-Shishtawy's Words

Strategic Oversight for a New Era: Integrating AI Security and Cyber Resilience into ESG Governance

Head of Cybersecurity Readiness, Cybersecurity Sector, Central Bank of Egypt

The financial landscape is shifting significantly. Environmental, Social, and Governance (ESG) criteria have evolved into a central pillar of corporate strategy, investment decisions, and customer trust. As financial institutions deploy Artificial Intelligence (AI) and digital technologies to drive innovation, a critical gap has emerged: the disconnect between cyber resilience and ESG governance.

While traditionally focused on Environmental (E) and Social (S) factors, ESG's Governance (G) pillar is fundamental. AI security is ensuring algorithms are fair, transparent, and resilient that is a core governance issue. Similarly, cyber resilience is the ability to prepare for, respond to, and recover from incidents which is directly measures operational resilience and sustainability. A cyber-resilient organization is more sustainable and well-governed, as its ability to protect customer data Social (S) and maintain critical infrastructure Environmental (E) under pressure reflects governance quality.

In Egypt's digital economy, effective governance requires robust oversight of cyber risk and secure AI deployment. A data breach or biased algorithm does more than cause financial loss, it erodes stakeholder and customer trust, damages reputation, and violates social responsibility, impacting all three ESG domains.

The Egyptian Financial sector stands at a focal point, navigating a digital transformation accelerated by sophisticated technologies like Artificial Intelligence (AI). This evolution, while promising major efficiency and customer experience benefits, expands the attack surface and introduces emerging risks.

As part of Central Bank of Egypt (CBE)'s Strategic Oversight directions to achieve its vision of building an integrated approach to enhance cybersecurity in the financial sector, this directive, materializing as the Egyptian Financial Cybersecurity Framework (EG Fin-CSF), establishes a robust foundation for **Governance, Risk Management, and Oversight (GRO)** model to emphasizes supervisory oversight role. The CBE enforces this approach through its Cybersecurity Readiness Oversight Program, a continuous cycle of assessment, auditing, assurance and follow-up for making cyber readiness a board-level metric. Complementing this, the Cyber Risk & Resilience Program quantifies inherent risk and measures cyber drill effectiveness, providing a clear view of sector maturity.

The anticipated update to the CBE's EG Fin-CSF is set to be a global pioneer, explicitly in this update the GRO model establishes a next-generation supervisory framework that will explore integration with AI security, automated oversight through SupTech-enabled monitoring, cross-border regulatory cooperation, and cyber resilience into ESG governance. This will mandate Financial institutions not only secure AI algorithms and data but also demonstrate how cyber resilience contributes to organizational sustainability and governance disclosures.

In conclusion: For Financial institutions, this means AI systems must be auditable and resilient, elevating cyber readiness from a technical metric to a critical governance indicator. The CBE's strategic oversight ensures that managing cyber risk and securing AI within an ESG context is mandatory, securing the stability of Egypt's financial ecosystem. For GRC leaders, a unified, enterprise-wide approach is non-negotiable as well as the cybersecurity and AI governance are central to corporate integrity and sustainability, aligning technology with long-term goals and building stakeholder confidence.

Lilian Magdy's Words

Sustaining and Developing the Professional Skills of the Internal Auditor

In an era defined by Artificial Intelligence (AI), automation, and accelerating regulatory change, Internal Audit is undergoing one of the most significant transformations in its history. The modern Internal Auditor is no longer viewed solely as an assurance provider, but as a strategic advisor, a technology-aware risk professional, and a trusted partner to executive management and the Board. To remain relevant, credible, and impactful, Internal Auditors must focus on Professional Skills Sustainability and Development. The Internal Auditors should continuously reflect on three fundamental questions:

1. What Are Professional Skills Sustainability and Development?

Professional Skills Sustainability refers to an auditor's ability to remain relevant, competent, and valuable over time despite continuous changes in technology. The Internal Auditor shall reflect a mindset of continuous adaptability and learning.

2. Why Should We Focus on Professional Skills, Sustainability and Development?

Focusing on skills sustainability is no longer optional as it is essential for individual auditors.

- Rapid Technological Disruption: AI, automation, and advanced analytics are reshaping control environments.
- Rising Stakeholder

Internal Audit Manager.

Expectations: Audit Committees, Boards, and regulators increasingly expect Internal Audit.

- Expanding Audit Scope: The Internal Audit mandate now routinely includes Digital transformation initiatives, ESG and sustainability reporting.
- Career Permanence and Professional Relevance: From an individual perspective, skills sustainability supports and Long-term employability.

3. How Can We Achieve Professional Skills Sustainability and Development?

Achieving sustainable professional skills requires a deliberate, structured, and continuous approach, at both the individual and Internal Audit function levels.

- Embed Continuous Learning: Integrate learning into daily work rather than relying solely on periodic training programs.
- Balance Digital and Human Skills: Combine technical and analytical expertise with strong communication, storytelling, influence, and ethical judgment.
- Personalized Skills Development: Maintain tailored development plans aligned with career goals, organizational strategy, and emerging risks.
- Strengthen Leadership Commitment: CAEs should lead by building diverse teams, encouraging innovation, investing in upskilling and continuous improvement.

Call to Action for 2026

Internal Auditors must embrace technology while strengthening human capabilities, ask the right questions, and invest in the right skills to ensure the profession's long-term relevance, credibility, and strategic value.

Maged Roshdy's Words

Digital Civilization: The Crisis of Value and the Quest for Wise Continuity

Technological evolution has reached a critical tipping point where its velocity outweighs our ability to control it. The pressing question is no longer just where we are going, but how can we continue wisely?

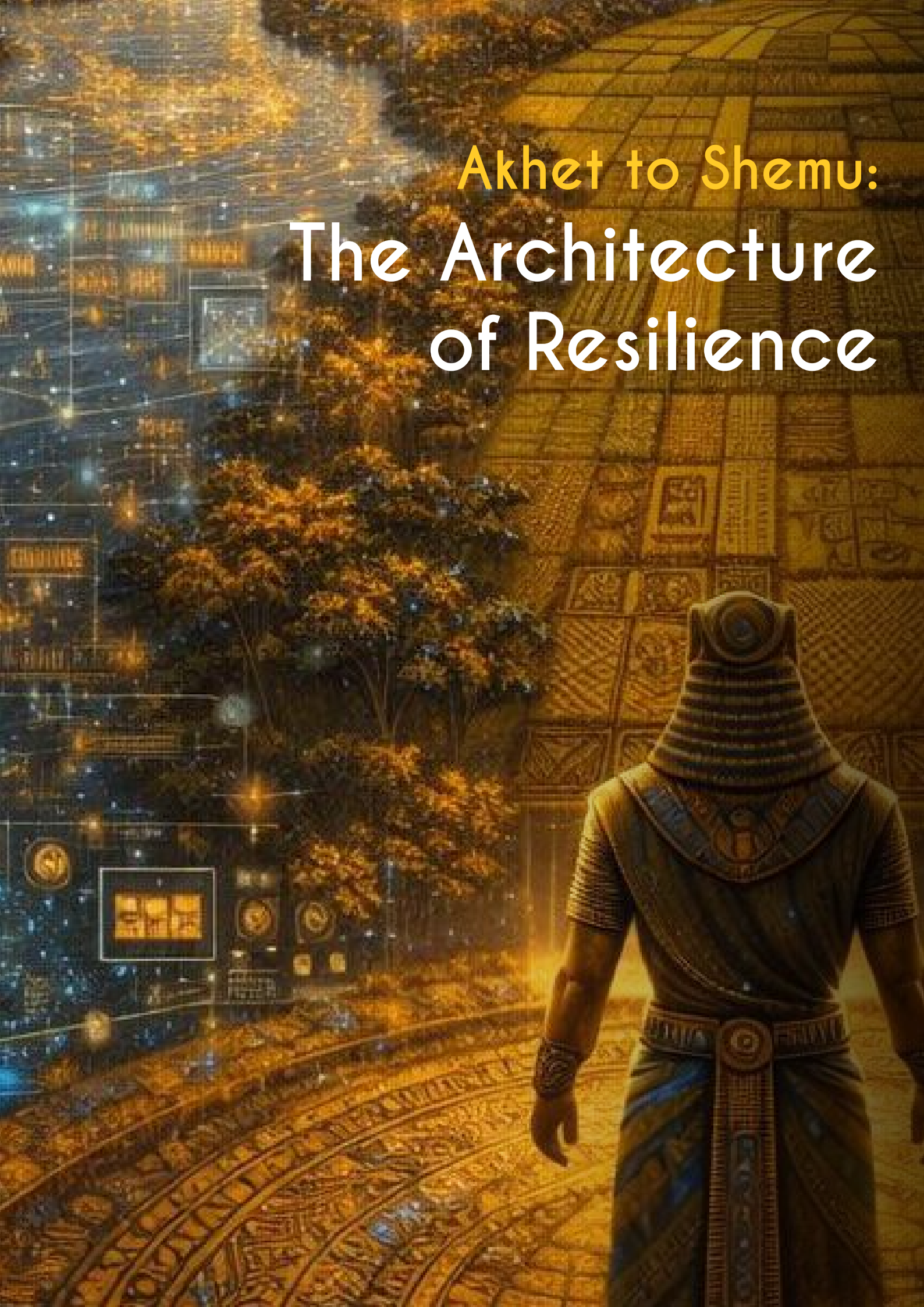
Manager of Information and Technology Security Management. Ambassador

The Inverted Pyramid: A Crisis of Meritocracy. Historically, civilization was built on a "natural selection" of merit: the educated and productive were rewarded, ensuring societal advancement. Today, this mechanism is collapsing. We are witnessing an "inverted" system where triviality is rewarded far more than craftsmanship. Consider the stark contrast between a medical engineer or a doctor—professions requiring years of gruelling effort and ethical responsibility—versus a "digital beggar" creating purposeless content. It defies social justice for the former to earn significantly less than the latter. This imbalance creates a "Parallel Economy," driving atypical inflation by pumping liquidity into valueless channels, marginalising true producers.

The Governance Gap: When Algorithms Outpace Law, Governance mechanisms are failing. Traditional, paper-based controls have no leverage in a borderless digital space. We cannot apply slow, manual audits to systems moving at light speed. While automation efforts exist, we lack a "Mother System"—a centralized international governance framework. Digital justice must be an inherent human right, much like international peace treaties, not a privilege for specific nations.

Cosmic Inspiration: Digital Physics Laws The solution lies in evolving our approach from mutable human regulations to immutable "Digital Physics Laws." We must establish "Code as Law" that functions with the certainty of gravity. I find no better model here than looking at the Universe itself: a system governed by strict, unbiased physical laws. Our digital ecosystem must be equally comprehensive, embedding integrity standards within the infrastructure itself, not treating them as an afterthought.

A Call to Guardians This economic deviation resembles a "cancer" growing without a genetic map, threatening societal collapse. I extend this call specifically to information security professionals. You are not just protecting data; you are the guardians of the genetic map for the next civilization. We must prioritize the continuity of the human race with wisdom that transcends abstract science. Let us make this possible before it is too late.


Akhet to Shemu:
The Architecture
of Resilience

The genius of Ancient Egypt was not only in its monuments, but in its understanding of rhythm. Akhet, Peret, and Shemu were never isolated events—they formed a continuous cycle of preparation, execution, and accountability. This same rhythm defines the most resilient organizations today. Governance sets direction before disruption arrives. Risk and compliance shape behavior as systems grow and complexity increases. Audit, cybersecurity assurance, and ESG reporting harvest truth, transparency, and trust at the end of the cycle.

Akhet reminds us that strong governance must anticipate uncertainty, not merely react to it. In a world of accelerating change, floods now arrive as cyber threats, regulatory shifts, and environmental pressures. Peret teaches that resilience is built through disciplined monitoring—where controls mature, risks are managed, and sustainability moves from promise to practice. Shemu completes the cycle by demanding honesty: outcomes must be measured, impacts disclosed, and lessons carried forward before the next cycle begins.

What the ancient Egyptians understood—perhaps better than we do—is that stability is not static. It is renewed, season after season, through structure, vigilance, and accountability. Modern frameworks for governance, risk, compliance, cybersecurity, audit, and ESG are not inventions of our time; they are evolutions of an ancient truth: systems survive when they respect cycles, prepare early, act deliberately, and learn continuously.

As the Nile once shaped a civilization, today's leaders must shape their organizations with the same discipline and foresight. The tools may have changed, but the principle remains eternal.

Order is not imposed once—it is cultivated, season by season.

GRC Summit Egypt

For Subscription Click Here

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

mag@grcsummiteg.com

www.grcsummiteg.com

grcsummit.eg grcsummit.eg grcsummit.eg