MAGAZINE

JANUARY 2025
ISSUED QUARTERLY
VOLUME 04

GRC EGYPT

IGNITE THE FUTURE.
LEAD WITH PURPOSE.
EMBRACE CHANGE.

Agile governance is more than a methodology – it's a commitment to continuous evolution. It represents our collective ability to transform uncertainty into opportunity, to see beyond current limitations and imagine extraordinary possibilities.

The future belongs to those who can navigate complexity with grace, intelligence, and unwavering strategic vision.

Engage

with industry leaders to gain insights into the latest trends and innovations in GRC, Audit, Cybersecurity, and ESG, ensuring you remain at the forefront of your field.

IGNITE THE FUTURE

Adaptive Leadership in Perpetual Evolution

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 2024

Ignite the Future.

Lead with purpose. Embrace change.

"Agile governance represents the quintessential paradigm of organizational excellence—a strategic commitment that transcends traditional methodological boundaries. It is the embodiment of institutional resilience, where adaptive intelligence meets purposeful vision, transforming complexity into a canvas of unprecedented opportunity. In an era of perpetual disruption, governance is no longer about maintaining the status quo, but about crafting a dynamic, forward-looking ecosystem that can anticipate, respond, and innovate with remarkable precision and strategic agility. This approach demands more than mere adaptability; it requires a holistic reimagining of organizational potential, where leadership becomes a fluid, contextual practice of continuous learning and strategic foresight. The true essence of agile governance lies not in controlling uncertainty, but in developing the organizational capacity to dance with complexity, turning potential challenges into strategic symphonies of innovation and growth.

Elin Hauge's Words

Digitalization Gone Astray


Chairperson of the Board
Wovv AS

Digitalization in general and artificial intelligence in particular is often proclaimed to be the solution to most, if not all, sustainability challenges. We tend to think that digital is sustainable, because the data are just flying wirelessly through the air.

There are indeed a vast number of highly valuable examples of how digital technologies solve important challenges, such as improved power utilization in production, better fish health in the aquaculture industry, and automated analysis of X-ray images in healthcare. However, the unpleasant reality is that all digital technologies leave significant and highly tangible physical footprints on our environment. The storage, transmission, and processing of data requires processing power. Generative artificial intelligence is particularly power-hungry. Electronic devices are also essential parts of the value chain, e.g. smartphones, wearables, industrial robots, servers, computers, monitors, etc. All these electronic devices come from somewhere, and when we are done with them, they go somewhere. The mining industry and waste management is intrinsically related to our digital transformation.

Let us dig into some more facts and details.

All things digital require physical hardware, such as smartphones, computers, servers, smartwatches, monitors, etc. All electronic devices require precious metals, which are obtained through physical mining. Many of these mines are either located in conflict zones, such as Russia and Congo, staffed by children, or in dire conflict with vulnerable ecosystems, such as the Norwegian plans for deep-sea mining.

All digital applications require electrical power. The explosion of generative artificial intelligence has led to a further brutal increase in the need for data centre capacity. According to the International Energy Agency, the data centre industry is on a trajectory to double the energy consumption from 2% of the total global energy consumption in 2022 to 4% in 2026, mostly due to generative artificial intelligence. That means that the global data centre industry alone is estimated to require as much electricity in 2026 as five times the current total electricity consumption of Egypt.

Even if the major cloud providers are working towards "net zero carbon footprint," the fundamental problem remains: insufficient production of sustainable electrical power. When big techs soak up all available green energy and carbon quotas, they are simply shifting the carbon problem to other players with less financial muscles. To meet the steeply increasing needs for electricity, all the major cloud service providers have recently announced heavy investments into nuclear power. Indeed, nuclear power is a key energy resource for the future, but is the development and expansion urged by the right drivers?

Access to clean drinking water is a geopolitical fire torch. In the frenzy to adopt digital technologies, it is easy to forget that the technology industry is a major consumer of clean water, both in the production of electronics and for cooling of data centres. Meta is building a new data centre in Toledo in Spain. This data centre is projected to require 660 million litres of water for cooling per year, in one of Europe's dryest regions.

Digital applications require devices. All commercially oriented hardware providers

in the market have recently launched high-profile marketing campaigns for the latest "AI-powered-something." When you buy new devices, what do you do with the relatively new and still very usable device that you no longer need? Less than one fifth of consumer electronics is recycled. The rest ends up in landfills, very often on the African continent, such as Agbogbloshie in Ghana. Child labour is not eradicated with digitalization, it just changes format. 18 million children are according to WHO currently at immediate health risk because they work in the informal waste management industry to dismantle smartphones and computers, a highly toxic job.

There are no silver bullets that can solve this imbalance between technological expansion and environmental footprints. However, we can all contribute:

- Keep electronic devices for longer. When you do need to replace them, make sure to either hand them off for restoration and a second life or make sure they are dispatched for recycling.
- Modesty in consumption is good for the planet, also when it comes to digital tools and content. Different generative artificial intelligence models (LLMs) have vastly different environmental impacts. Choose wisely.
- Efficient code used to be a quality stamp of experienced developers. Build a culture for efficient software engineering in your company, including the AI teams.
- Include the environmental footprint of your digital transformation efforts into the sustainability reporting to promote transparency and awareness.

The digitalisation toolbox is just that, a toolbox. Artificial intelligence constitutes a key part of this toolbox, but it is by no means sustainable per se. Whether it becomes an environmental villain, or a saving angel depends on how we choose to apply the toolbox. It is high time to make conscious choices.

"Digital transformation holds immense promise, but its sustainability lies in our choices. Let innovation be a force for progress, balanced by responsibility to our planet and future generations."

Hani Barrada's Words

Choose Your Tribunal, Set the Rules: Why Arbitration Is the Future of Dispute Resolution


Founder & Managing Partner
Barrada Law Office

Arbitration Agreement

Arbitration agreements are generally divided into two types:

- Agreements providing that if a dispute should arise, it will be resolved by arbitration. These will generally be normal contracts, but they contain an arbitration clause
- Agreements that are signed after a dispute has arisen, agreeing that the dispute should be resolved by arbitration

Agreements to refer disputes to arbitration are generally presumed to be separable from the rest of the contract. This means that an issue of validity pertaining to the contract as a whole will not automatically vitiate the validity of the agreement to arbitrate.[5] For example, in disputes on a contract, a common defense is to plead the contract is void, and thus any claim based upon it fails. It follows that if a party successfully claims that a contract is void, then each clause contained within the contract, including the arbitration clause, would be void.
This protects the tribunal's ability to arbitrate beyond the termination of the contract. Arguably, it is necessary to ensure that disputes are arbitrated rather than litigated -- without such a clause, a dispute arising out of a contract will necessarily be litigated.
Arguably, either position is potentially unfair; if a person is made to sign a contract under duress, and the contract contains an arbitration clause highly favorable to the other party, the dispute may still referred to that arbitration tribunal. Conversely, a court may be persuaded that the arbitration agreement itself is void having been signed under duress. However, most courts will be reluctant to interfere with the general rule which does allow for commercial expediency; any other solution (where one first had to go to court to decide whether one had to go to arbitration) would be self-defeating.

International Enforcement

It is often easier to enforce arbitration awards in a foreign country than court judgments. Under the New York Convention 1958, an award issued in a contracting state can generally be freely enforced in any other contracting state, only subject to certain, limited defenses. Only foreign arbitration awards are enforced according to the New York Convention. An arbitral decision is foreign where the award was made in a state other than the state of recognition or where foreign procedural law was used.[43] In most cases, these disputes are settled with no public record of their existence as the loser complies voluntarily,[44] although in 2014 UNCITRAL promulgated a rule for public disclosure of investor-state disputes.[44]
Virtually every significant commercial country in the world is a party to the Convention while relatively few countries have a comprehensive network for cross-border enforcement of judgments in their courts. Additionally, the awards are not limited to damages. Whereas typically only monetary judgments by national courts are enforceable in the cross-border context, it is theoretically possible (although unusual in practice) to obtain an enforceable order for specific performance in an arbitration proceeding under the New York Convention.
Article V of the New York Convention provides an exhaustive list of grounds on which enforcement can be challenged. These are generally narrowly construed to uphold the pro-enforcement bias of the Convention.

Arbitral Tribunal

The arbitrators who determine the outcome of the dispute are called the arbitral tribunal. The

composition of the arbitral tribunal can vary enormously, with either a sole arbitrator sitting, two or more arbitrators, with or without a chairman or umpire, and various other combinations. In most jurisdictions, an arbitrator enjoys immunity from liability for anything done or omitted whilst acting as arbitrator unless the arbitrator acts in bad faith.
Arbitrations are usually divided into two types: ad hoc arbitrations and administered (or institutional) arbitrations.
In ad hoc arbitrations, the arbitral tribunals are appointed by the parties or by an appointing authority chosen by the parties. After the tribunal has been formed, the appointing authority will normally have no other role and the arbitration will be managed by the tribunal.
In administered arbitration, the arbitration is administered by a professional arbitration institution providing arbitration services, such as the LCIA in London, the ICC in Paris, or the American Arbitration Association in the United States. Normally the arbitration institution also will be the appointing authority. Arbitration institutions tend to have their own rules and procedures and may be more formal. They also tend to be more expensive, and, for procedural reasons, slower.

Duties of the Tribunal

The duties of a tribunal will be determined by a combination of the provisions of the arbitration agreement and by the procedural laws which apply in the seat of the arbitration. The extent to which the laws of the seat of the arbitration permit "party autonomy" (the ability of the parties to set out their procedures and regulations) determines the interplay between the two.
However, in almost all countries the tribunal owes several non-derogable duties. These will normally be:

- to act fairly and impartially between the parties, and to allow each party a reasonable opportunity to put their case and to deal with the case of their opponent (sometimes shortened to comply with the rules of natural justice; and
- to adopt procedures suitable to the circumstances of the particular case, so as to provide a fair means for resolution of the dispute.[48]

Arbitral Awards

An arbitral Award merely includes both a final award and an interim award. Although arbitration awards are characteristically an award of damages against a party, in many jurisdictions, tribunals have a range of remedies that can form a part of the award. These may include:

- payment of a sum of money (conventional damages)
- the making of a "declaration" as to any matter to be determined in the proceedings
- in some jurisdictions, the tribunal may have the same power as a court to:
  1. order a party to do or refrain from doing something ("injunctive relief")
  2. to order specific performance of a contract
  3. to order the rectification, setting aside, or cancellation of a deed or other document.
  4. In other jurisdictions, however, unless the parties have expressly granted the arbitrators the right to decide such matters, the tribunal's powers may be limited to deciding whether a party is entitled to damages. It may not have the legal authority to order injunctive relief, issue a declaration, or rectify a contract, such powers being reserved to the exclusive jurisdiction of the courts.

Ashraf Hamasa's Words

Unlocking the Potential for Clean Energy

2024 is set to be the hottest year ever recorded. Global emission from fossil fuels have reached a record high. There is a significant amount of work to do to decarbonize. In November, G20 leaders called for increased climate finance from "billions to trillions". In COP29, annual funding for developing states tripled to $300 billion by 2035.

Delegations also agreed on rules for carbon credits. We think the solution to balance security, affordability, and sustainability in energy systems is relatively clear. We must increase our reliance on renewables, leverage gas to accelerate the energy transition and expand grid infrastructure. Step by step, this plan will help us achieve the energy transition.

Renewable Energy: The Cornerstone of Decarbonization

The world needs renewable energy sources like wind and solar, as well as solutions like green hydrogen which can be used to store and transport renewable electricity, to decarbonize. Globally, Siemens Energy have installed around 117GW of renewable energy capacity since 1998, enabling our customers to reduce their carbon footprint by approximately 329 million tons per year, which is the equivalent of taking approximately 71.5 million cars off the road per year.

When maximally utilized, renewable energy sources will play an indispensable role in helping Egypt achieve its

Managing Director
Siemens Energy in Egypt

vision of increasing its energy mix by 42% by 2030. Looking at the Lekela Egypt 250 MW wind farm in Ras Ghareb, for example, we see that it produces over 1,000 GWh of electricity each year, supplying power to more than 350,000 homes and decreasing CO2 emissions by about 550,000 tons annually.

This is just one of the many reasons driving Siemens Energy's commitment to decarbonize its operations by 2030. Drawing from our experience, we can confirm that decarbonization is effective. After installing 3,280 solar PV panels covering approximately 8,500 square meters of our Egypt Service Center's roof in Ain Sokhna, we have witnessed a reduction in our carbon footprint by around 1,600 tons per year. These panels, with a capacity of 1.9 MW, provide 90% of the service center's annual electricity needs, totaling 3 GWh per year.

The Role of Gas in the Energy Transition

Despite record growth in renewables in recent years, the world needs gas turbines to continue to meet energy demands. We know that the shift from coal to gas would cut CO2 emissions by 50%, especially that our various solutions can increase efficiency and reduce CO2 emissions.

In Egypt, we have collaborated with our partners to provide electricity to 40 million Egyptian people through the completion of the world's three largest gas-fired combined cycle power plants (4.8GW each) in Beni Suef, Burullus and the New Administrative Capital. The multi-year agreement including the operations and maintenance of the three power plants, covers all on-site equipment including 24 gas turbines, twelve steam turbines, 36 generators and 24 heat recovery steam generators.

Furthermore, the establishment of gas-insulated switchgear substations throughout the country has facilitated reliable

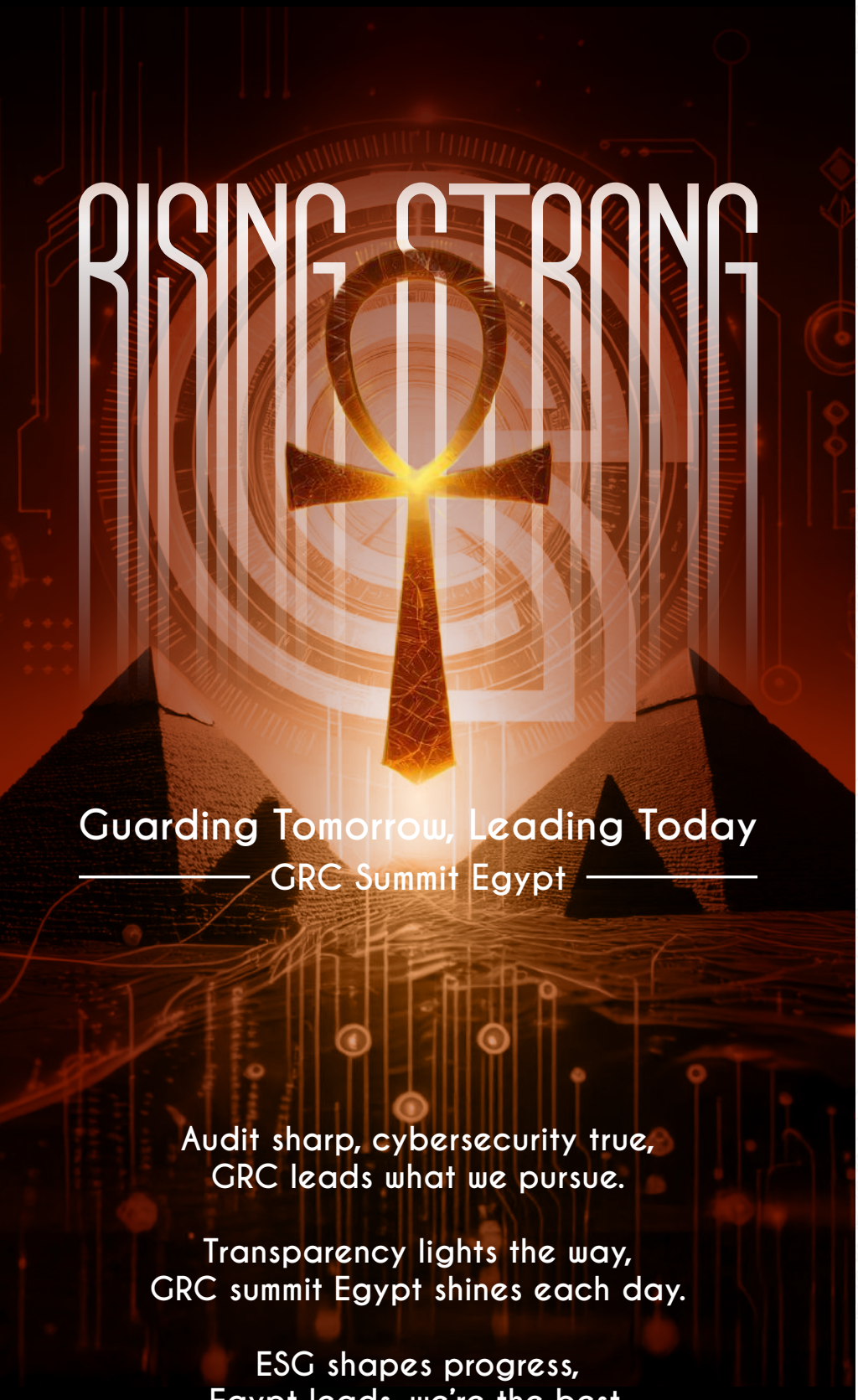
energy transmission.

Empowering Grids for a Sustainable Future

The diversification of energy sources, widely known as the energy mix, necessitates the strengthening of electrical grids. There is no transition without transmission. Today's electricity grids are not prepared to meet the rapidly evolving demands of the future, whether in terms of new capacity or the flexibility required to accommodate the evolving energy mix, which will include a large amount of intermittent electricity sources. The challenge is immense, especially in developing countries. Public-private partnerships are crucial to establish reliable, efficient transmission networks capable of meeting future energy needs.

Leading the Change, Together

Transitioning to a sustainable future is a collective endeavor. To accelerate the shift to clean energy ,we need the support of various stakeholders, including policymakers, the public, and industry partners. Regulatory reforms that streamline the deployment of clean energy are essential. Additionally, individual actions, such as adopting sustainable practices in daily life – and spreading the sustainability culture among family members and friends – can significantly reduce carbon emissions and contribute to a healthier planet for future generations.



In today's rapidly evolving business landscape, the integration of Artificial Intelligence (AI) into Governance, Risk, and Compliance (GRC) frameworks is becoming increasingly essential. AI offers transformative potential, enabling organizations to enhance their GRC processes through improved efficiency, accuracy, and proactive risk management.

Enhancing Governance

AI can significantly improve governance by automating routine tasks and providing deeper insights into organizational operations. Machine learning algorithms can analyze vast amounts of data to identify patterns and anomalies that might indicate governance issues. For instance, AI-driven analytics can monitor compliance with internal policies and external regulations, ensuring that any deviations are promptly

Ramy Abbas's Words

Practical Implementation of AI in Governance, Risk, & Compliance (GRC)

flagged for review. This not only streamlines governance processes but also ensures a higher level of transparency and accountability.

Strengthening Risk Management

Risk management is a critical component of GRC, and AI plays a pivotal role in enhancing its effectiveness. Traditional risk management approaches often rely on historical data and manual assessments, which can be time-consuming and prone to human error. AI, on the other hand, can process real-time data from various sources, providing a dynamic and comprehensive view of potential risks. Predictive analytics powered by AI can forecast future risks based on current trends, allowing organizations to take proactive measures to mitigate them. This shift from reactive to proactive risk management can significantly reduce the likelihood of adverse events and their associated costs.

Streamlining Compliance

Compliance with regulatory requirements is a complex and ongoing challenge for many organizations. AI can simplify this process by automating compliance monitoring and reporting. Natural Language Processing (NLP) algorithms can scan and interpret regulatory documents, ensuring that all relevant requirements are identified and addressed. Additionally, AI can continuously monitor business activities and transactions, automatically flagging any that may violate compliance standards. This not only reduces the burden on compliance teams but also minimizes the risk of non-compliance penalties.

Practical Implementation Steps

- **Assessment and Planning:** Begin by assessing the current GRC framework and identifying areas where AI can add value. Develop a clear implementation plan that outlines objectives, timelines, and resource requirements.
- **Data Integration:** Ensure that all relevant data sources are integrated into the AI system. This includes internal data (e.g., financial records, operational data) and external data (e.g., regulatory updates, market trends).
- **Algorithm Development:** Develop and train AI algorithms tailored to the specific needs of the GRC framework. This may involve collaboration with AI experts and data scientists.
- **Pilot Testing:** Conduct pilot tests to evaluate the effectiveness of the AI system in real-world scenarios. Use feedback from these tests to refine and improve the system.
- **Full Deployment:** Once the AI system has been thoroughly tested and refined, proceed with full-scale deployment. Ensure that all relevant stakeholders are trained on how to use the system effectively.
- **Continuous Monitoring and Improvement:** AI systems require ongoing monitoring and maintenance to ensure they remain effective. Regularly update the algorithms and data sources to reflect changing conditions and new regulatory requirements.

Conclusion

The practical implementation of AI in GRC offers numerous benefits, including enhanced governance, more effective risk management, and streamlined compliance processes. By leveraging AI, organizations can not only improve their GRC frameworks but also gain a competitive edge in an increasingly complex and regulated business environment. As AI technology continues to advance, its role in GRC will undoubtedly become even more integral, driving further innovation and efficiency.

Marwa Abdel Latif's Words

Working in an agile environment

Compliance and Data privacy

The simplest way to engross the various definitions for 'data privacy', is that the mainstream community needs to know what personal data organizations are collecting about them and how they are using it. Of course, this a simplistic way to look at the topic but it is useful to set the scene. Data privacy is far more than just the security and protection of personal data. It all simmers down to how organizations are using that personal data. The landscape is complex and it continues to evolve when it comes to data privacy. The Banking Sector needs to process personal data in an ethical and legal manner, without bombarding customers. It could also simply put by not sharing personal information with third parties without the customer's consent. Many banks have recognized the significant risks of cyber-attacks and data breaches alongside to continuous and sleepless trials to safeguard customers' data. This has increased awareness about the importance of data privacy and protection.
One of the key principles of data privacy is to establish the foundation that involves setting access controls to protect information from unauthorized parties, getting consent from data subjects when necessary, and maintaining data integrity. Data privacy needs to be a top priority for businesses.

Failure to comply with data privacy regulations can lead to unnecessary wounds. Complying with data privacy laws is not something that can be left to the legal and compliance departments alone. Compliance with data privacy laws requires that one and all in banks understand their responsibilities to protect personal data. It is vital to communicate your data privacy policies and practices to your customers and employees to ensure they are familiar with how to process and protect personal data.

Agile Governance

Agile governance lands on a set of core agile values, behaviors and practices that allows all banks to prosper in a world characterized by volatility, uncertainty, complexity and ambiguity. Governance impacts how banks' objectives are set and achieved, how risk is managed and how performance is optimized. It can be defined as the structures and processes for decision-making and accountability.
It's characterized by demonstrating control through transparency through multiple policies and processes that targets the elevation of the overall performance in a way that's consistent at all levels and aspects within banks.
The concept of consistency of governance across such a broad spectrum is at an early stage of its evolution.
The goal and term agile governance refer to how banks would oversee, monitor, and guide its businesses correlated with agile projects. It can apply to a single agile project, but more often describes the governance framework for the organization's full portfolio.
The alignment of both, is the key to a viable development and it mandates from both business and organizational levels correspondingly highly effective and responsive governance in order to deliver value to the business.
This article is composed to portray for banks the mainstay to benefit from agile methodologies, mitigating risks and ensure strategic alignment.

The *Rhythm* of Excellence: GRC Summit Egypt

At the core of progress lies the dynamic interplay of governance, risk, and compliance (GRC)—an evolving blend of disciplines that shape the future of industries and nations. The GRC Summit Egypt brings together the pillars of Audit, ESG, Cybersecurity, Risk Management, Compliance, and Fraud Detection with the transformative power of digitalization and data innovations driving global change.

From the timeless legacy of Egypt's pyramids to the cutting-edge streams of artificial intelligence, the country leads with visionary governance that blends its ancient wisdom with modern ingenuity. Each summit session embodies a commitment to progress, integrity, and excellence.

- Audit illuminates truth, fostering trust through transparency.
- ESG guides the way to a sustainable future, where both the earth and governance thrive.
- Cybersecurity shields the digital frontier, securing innovation's path forward.
- Risk Management provides steady guidance amid challenges, empowering bold choices.
- Compliance aligns actions with core principles, building a foundation of trust.
- Fraud Detection uncovers deception, ensuring justice prevails.
- Data Analytics uncovers insights that spark success.

As Egypt continues to rise, it stands as a beacon of resilience and leadership, seamlessly blending technology and tradition to redefine GRC on the global stage. This summit represents more than an event—it's a movement to inspire action, empower change-makers, and ignite the future.

Transformation is a journey, not a destination. It thrives on the synergy between human ingenuity and technological advancement—where governance navigates complexity, risk becomes opportunity, and compliance drives unparalleled global progress. True leadership lies not in preserving the status quo, but in our ability to reimagine possibilities and create futures once thought impossible.

Senior Sustainable Finance and SDGs Expert

Perihan Abdelghaly's Words

Assessing the Role of Risk Management & Compliance for Greater Sustainability & Success

As global demands for sustainable business practices grow, the MENA region, including Egypt, is accelerating efforts to embed Environmental, Social, and Governance (ESG) principles across sectors. For countries within this region, risk management and compliance play pivotal roles in achieving not just sustainability goals but also long-term economic resilience. Egypt's Sustainable Development Strategy (SDS) 2030 exemplifies a national roadmap towards economic, social, and environmental balance, while frameworks like Saudi Vision 2030 and the UAE's Net Zero by 2050 accentuate MENA's commitment to sustainable development. However, the path to sustainability is not straightforward. From climate vulnerabilities to financial uncertainties, the region faces diverse challenges that require meticulous risk management and robust compliance structures. By understanding the synergies between risk management, compliance, and sustainability, Egypt and MENA can unlock greater economic success and environmental resilience.

The Current Landscape of Risk Management and Compliance in Egypt and the MENA Region reflects critical changes that require a due attention. Egypt, along with other MENA nations, is actively refining its regulatory landscape to align with global sustainability standards. Over recent years, Egypt has enacted several environmental and social regulations to support sustainable development and protect its natural resources, emphasizing regulatory updates on ESG disclosures and green finance. Meanwhile, Saudi Arabia and the UAE have made substantial investments in clean energy and are introducing policies to reduce their dependency on oil revenues, signalling a fundamental shift towards sustainable growth.

However, the region's sustainability journey is challenged by geopolitical instability, resource dependence, and economic volatility. For instance, Egypt's water scarcity and regional conflicts present risks that must be managed to achieve long-term sustainability. Adopting risk management strategies and compliance frameworks can help mitigate these risks, attracting international investment and fostering more resilient economies.

Why Risk Management and Compliance Are Critical for Sustainability? Effective risk management identifies and addresses the unique environmental, social, and governance risks that companies face, especially in a climate-vulnerable and resource-limited region like MENA. For businesses, managing climate risks, financial volatility, and regulatory requirements ensures not only compliance but also resilience. Compliance, meanwhile, is crucial for maintaining credibility with global investors, many of whom are now prioritizing investments in companies that align with international ESG standards.
A prime example is the recent green finance policies implemented by the Central Bank of Egypt, which mandate that financial institutions incorporate ESG considerations into their operations and lending practices. These regulations improve the environmental performance of banks and ensure they contribute to the national sustainability agenda. Across MENA, companies are finding that integrating these frameworks supports compliance and increases resilience against emerging risks.

Key Areas of Focus in Risk Management for Sustainable Business Practices

- **Climate Risk:** Climate risk is a major concern for Egypt and other MENA countries, where rising temperatures and water scarcity are prominent issues. By assessing and mitigating these risks, companies can prevent disruptions and reduce operational costs. Egypt, in particular, is focusing on risk management frameworks to address water scarcity and adapt to rising climate threats, which, if left unmanaged, could undermine economic stability.
- **Environmental and Social Risks:** Managing ESG risks requires addressing pollution, resource management, and labour rights in ways that align with local needs. Effective environmental risk management policies improve resource efficiency and reduce pollution, while social risk management enhances employee welfare and community engagement, which can be critical in regions with significant social disparities.
- **Financial Risk and Transparency:** Transparent financial reporting has become increasingly important for attracting sustainable investments. For instance, adopting global reporting standards like GRI, TCFD, and IFRS helps MENA banks improve transparency, meet compliance, and strengthen investor confidence. As regional economies aim to attract foreign capital, these standards provide the assurance that investors seek in emerging markets.

Role of Compliance in Enhancing Sustainability in the MENA Region

- **Environmental Regulations and Compliance:** Environmental regulations are crucial to achieving sustainability in the MENA region. Egypt, for example, has implemented stringent regulations around pollution control and natural resource conservation. Compliance with these regulations not only reduces environmental impact but also aligns companies with national sustainability targets.
- **Social Responsibility Compliance:** Labour rights, anti-corruption measures, and corporate governance standards are increasingly integrated into the region's regulatory frameworks. By complying with these standards, companies can prevent social risks and improve public trust, crucial for long-term success in a market where social inequality and corruption can impact growth.
- **International Standards and Certifications:** Certifications like ISO 14001 for environmental management and ISO 45001 for occupational health and safety bolster a company's credibility with investors. By adopting these standards, companies in the MENA region can demonstrate their commitment to sustainability, which can enhance their reputation and open doors to new markets.

Case Studies from Egypt and MENA Region: Success Stories and Challenges

- **Egypt's Central Bank and Sustainable Finance:** The Central Bank of Egypt (CBE) has introduced policies that require banks to incorporate sustainability into their lending practices, significantly impacting the financial sector's role in sustainable development. By focusing on green finance and climate resilience, CBE has set a benchmark in the region. However, smaller banks face challenges in implementation due to limited resources, highlighting the need for more accessible frameworks and tools.
- **Saudi Banks and ESG Risk Management:** Saudi Arabian banks have made strides in integrating ESG risk management within their operations. With initiatives focused on climate and social risk, these banks have attracted foreign investment while meeting national sustainability goals. Although challenges remain, including the high costs of ESG compliance, Saudi banks are demonstrating the long-term benefits of aligning with global standards.

The Impact of Risk Management and Compliance on Long-Term Success and Investor Confidence

For companies in the MENA region, particularly in Egypt, building strong risk and compliance frameworks is essential for attracting foreign investment and improving financing conditions. Companies with robust ESG practices enjoy higher investor confidence, better financing terms, and greater resilience against disruptions. This relationship between ESG compliance and investment is increasingly evident, with more MENA companies securing green financing as they prioritize sustainability and transparency.

For example, Egyptian companies that adhere to GRI standards and IFRS reporting have seen improved access to capital markets. This trend is encouraging more companies in the region to adopt similar standards, strengthening their market positioning and enabling long-term growth.

Future Outlook and Strategic Recommendations

As the region continues to focus on sustainability, technological advancements in data analytics and AI can strengthen risk management and compliance. By leveraging these tools, companies can make data-driven decisions that enhance ESG performance, streamline reporting processes, and improve transparency. To fully realize these benefits, MENA companies and governments should prioritize the following strategies:

- **Develop Robust ESG Compliance Frameworks:** This includes integrating climate risk assessment, biodiversity protection, and social responsibility measures into business operations.
- **Enhance Collaboration between Public and Private Sectors:** Governments and private entities should work together to create a regulatory environment conducive to sustainable growth.
- **Invest in Training and Resources for SMEs:** Small and medium enterprises (SMEs) require resources to adopt ESG standards, which can include government-sponsored training programs and accessible reporting tools.
- **Encourage Regional Sustainability Standards:** By promoting shared sustainability standards across the MENA region, companies can benefit from consistency in regulatory requirements, fostering a sustainable regional economy.

Conclusion: Moving Toward a Sustainable, Resilient Future in MENA through Risk Management and Compliance

As Egypt and other MENA countries embrace sustainability, the role of risk management and compliance becomes increasingly vital. By aligning with global ESG standards, managing climate and social risks, and adhering to local regulations, companies in the region can build resilience, attract investment, and create long-term value. These strategies not only ensure compliance but also strengthen the foundation for a sustainable future, making risk management and compliance indispensable tools for regional success.

“Effective risk management and compliance are the pillars of sustainable growth in the MENA region. By aligning with global ESG standards and addressing local challenges like climate risk and social disparities, businesses can unlock long-term economic resilience, enhance investor confidence, and contribute to the region’s sustainable future.”

Hesham ElGindy's Words

Strategies to successfully navigate GRC and secure a Win-Win with Internal Audit

Governance, Risk, and Compliance (GRC) and Internal Audit are closely related concepts that play crucial roles in an organization's overall risk management and governance.
Improving the integration between GRC and Internal Audit can enhance overall effectiveness and efficiency in managing risks and ensuring compliance among many other very important benefits.
Although successful separation of GRC from internal audit is evident in several organizations that have effectively maintained distinct functions while promoting collaboration, separating GRC from internal audit may present several challenges such as Cultural Resistance, Communication Gaps, Role Clarity, Resource Allocation, Integration of Processes and Management Buy-In.
However, I'm still a true believer that separating GRC and internal audit will enhance the overall effectiveness of both functions and the organization as a whole.

Additionally, mixing GRC and Internal Audit can lead to conflicts of interest, unclear responsibilities and diluted effectiveness. Maintaining their separation allows each function to operate independently, ensuring that governance, risk management, compliance, and audit processes are robust and effective. This separation ultimately contributes to a stronger overall risk management and governance culture within the organization

Interrelations between both functions can be seen in the following:

- Collaboration: Internal audit functions often collaborate with GRC teams to ensure a holistic view of risk and compliance across the organization.
- Assessment: Internal auditors evaluate the effectiveness of GRC processes, providing recommendations for enhancing governance and compliance frameworks.
- Continuous Improvement: Findings from internal audits can inform GRC strategies, leading to better risk management practices and compliance efforts.
- Reporting and Accountability: Both internal audit and GRC initiatives emphasize accountability and transparency, ensuring that stakeholders are informed about risk and compliance issues.

The following are some suggested strategies to foster better integration between both functions:

- **Establish Clear Communication Channels**
  1. Regular Meetings: Schedule ongoing meetings between internal audit and GRC teams to discuss findings, risks, and compliance updates.
  2. Shared Platforms: Use collaboration tools or shared platforms for documentation and reporting to enhance transparency and information sharing.


Group Vice President - Governance, Risk and Compliance
TAQA

- **Align Objectives and Goals**
  1. Common Objectives: Ensure both teams work towards shared organizational goals, such as risk mitigation and compliance adherence.
  2. Unified Framework: Develop a unified governance framework that incorporates both internal audit and GRC perspectives

- **Cross-Functional Training**

1. Skill Development: Provide training sessions that cover both internal audit and GRC concepts to foster understanding of each other's roles.
2. Job Shadowing: Encourage team members to shadow each other to gain insights into processes and challenges.

- **Risk Assessment Collaboration**
  1. Joint Risk Assessments: Conduct joint risk assessments to identify and prioritize risks effectively, leveraging the expertise of both teams.
  2. Shared Risk Registers: Maintain a single risk register that is accessible to both internal audit and GRC for better tracking and accountability.

- **Integrated Reporting**
  1. Coordinated Reporting: Develop integrated special purpose reports that combine findings from both internal audit and GRC activities, providing a comprehensive view of the organization's risk landscape.
  2. Dashboard Creation: Utilize dashboards that highlight key metrics relevant to both areas, facilitating real-time decision-making.

- **Leverage Technology**
  1. GRC Software: Implement GRC software that supports both internal audit and compliance functions, ensuring data consistency and accessibility.
  2. Data Analytics: Use data analytics tools to improve risk identification and assessment, enhancing both internal audit and GRC processes.

- **Foster a Culture of Collaboration**
  1. Encourage Teamwork: Promote a culture where collaboration between internal audit and GRC is valued and recognized.
  2. Celebrate Successes: Acknowledge joint achievements to reinforce the importance of integration.

- **Continuous Improvement**
  1. Feedback Mechanisms: Establish feedback loops for both teams to assess the effectiveness of integration efforts and identify areas for improvement.
  2. Regular Reviews: Conduct regular reviews of integration processes and adjust strategies as needed to ensure alignment with organizational objectives.

By implementing these strategies, organizations can strengthen the integration between GRC and internal audit, leading to a more cohesive approach to governance, risk management and compliance. This collaborative effort not only enhances accountability but also supports the organization's overall strategic goals. With all that being said, GRC and Internal Audit are crucial components of an organization's framework for ensuring effective management and accountability. Both functions, Enhanced Decision Making, Risk Mitigation Regulatory Compliance, Operational Efficiency, Internal Control Strengthening and Alignment with Strategic Goals.

In conclusion, GRC and Internal Audit are integral to an organization's health and sustainability. They not only protect the organization from risks but also promote a culture of governance and accountability, ultimately contributing to long-term success.

Nadine Kamal's Words

Elevating Data Privacy: How Identity and Access Management (IAM) Drives High-Impact Privacy and Compliance for Organizations

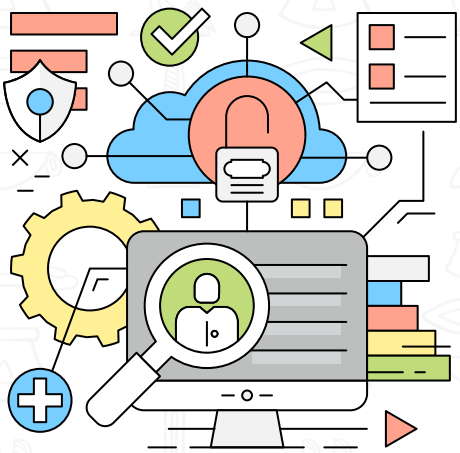
In the era of virtualization, organizations face tremendous challenges in protecting information assets while as ensuring regulatory compliance. With the rise in cyberattacks, privacy laws such as GDPR, INCDPA, and PIPL have become stricter, driving the development of frameworks like COBIT, ISO 27001, NIST, and APEC to guide organizations in safeguarding data.

A key tool in managing data privacy and protection is Identity and Access Management (IAM). Successful IAM begins with data classification and inventory, helping organizations understand what data they have, where it resides, and who can access it.

Let's talk about IAM, what is IAM……, Identity and Access Management is a framework of policies, technologies, and practices that help organizations manage and secure access to digital resources. It ensures that only authorized individuals can access and controlling who can access what, under what conditions, in what layer in the system and for how long.

There is a deep connection

between **IAM and Data** Privacy, the core of data privacy lies in protecting personal and sensitive information. IAM plays a critical role in data privacy by helping organizations implement the "need-to-know" principle, limiting access to sensitive data. This reduces the risk of unauthorized exposure and potential breaches.



Key Features of IAM Supporting Privacy and Compliance:

- **User Authentication:** Strong mechanisms like multi-factor authentication (MFA) ensure only legitimate users can access systems, reducing breach risks.

- **Role-Based Access Control (RBAC):** Access is granted based on users' roles, ensuring employees, contractors, and partners only access the data needed for their job functions

  Examples of RBAC include:

  1. Basic Access Roles (e.g., email, general access)
  2. Business Access Roles (e.g., sales, controlling, warehouse)
  3. Technical Roles (e.g., system administration)
  4. Auditor Roles (e.g., limited to the audit duration)

The RBAC access also addresses a deeper layer under the transactions layer, sublayers access control such as "object access, info type access, company code access".

- **Effective multiple controls such as**
  1. Password, it's complexity & having validity period for renewing.

2. Review over terminated users periodically and see the last login date with the termination date and if anything is identified a gap analysis must be performed & have a corrective action.
3. Review of critical access periodically, this is one of the very crucial controls.
4. Review of the access itself periodically performed to show is any changes on the user / employee job profile.

- **Automated Provisioning and De-provisioning:** Automated workflows ensure timely access granting and revocation, reducing human error.

- **Identity Governance:** Ensure that user identities are properly managed throughout their lifecycle. From onboarding to offboarding, IAM ensures that access rights are granted, modified, or revoked in line with organizational policies, minimizing the risk of improper access.

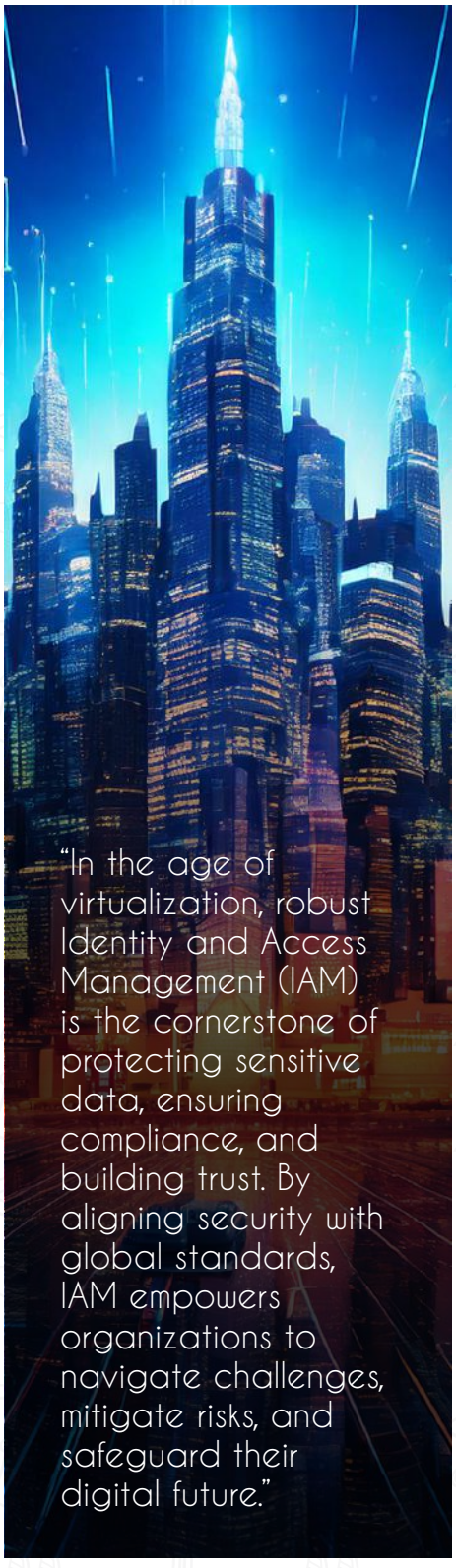
- **Compliance Integration:** Align IAM practices with industry regulations by adopting frameworks such as NIST, ISO 27001, and others. This integration should be reflected in the organization clear Policies, Processes, Procedures to guide & govern the IAM within the organization & is in line with regulatory. These Policies & Procedures must be updated annually, a process for an annual walkthrough is mandatory.

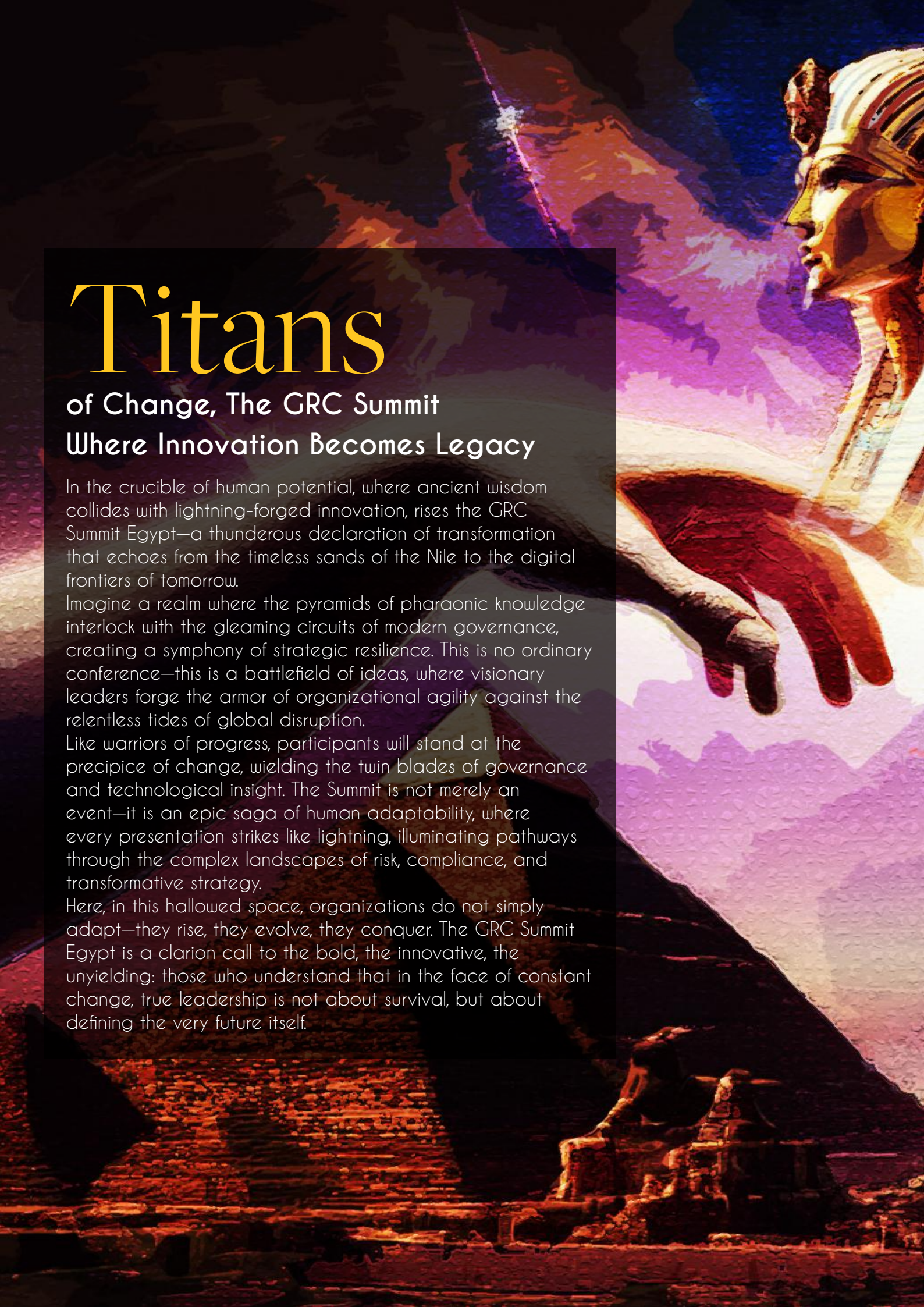
- **Employee Training and Awareness:** Ongoing employee education about security best practices, data privacy, and the organization's policies, processes & procedures is essential. There are Initiatives like Zero-Trust architecture, Information Security Awareness Month and Mind-well-being to have more focus on threats that help keep security top-of-mind.

- **Audit Trails and Monitoring:** Continuous monitoring and audit logs track who accessed data, when, and why, enabling quick response to potential data privacy violations.

Having said the above and by having automated and centralized IAM, organizations can better manage identities and access rights, reducing complexity and administrative burdens. IAM also integrates with other security measures like encryption and threat detection, enhancing overall cybersecurity.

The Conclusion; As data privacy continues to be a priority, especially with AI advancements, organizations must prioritize robust IAM practices. By doing so, they can protect sensitive information, comply with regulations, and maintain customer trust in a complex digital landscape.
By implementing a comprehensive IAM strategy, organizations can mitigate risks, enhance privacy protection, and maintain customer trust in an increasingly complex regulatory environment.





Titans

of Change, The GRC Summit Where Innovation Becomes Legacy

In the crucible of human potential, where ancient wisdom collides with lightning-forged innovation, rises the GRC Summit Egypt—a thunderous declaration of transformation that echoes from the timeless sands of the Nile to the digital frontiers of tomorrow.

Imagine a realm where the pyramids of pharaonic knowledge interlock with the gleaming circuits of modern governance, creating a symphony of strategic resilience. This is no ordinary conference—this is a battlefield of ideas, where visionary leaders forge the armor of organizational agility against the relentless tides of global disruption.

Like warriors of progress, participants will stand at the precipice of change, wielding the twin blades of governance and technological insight. The Summit is not merely an event—it is an epic saga of human adaptability, where every presentation strikes like lightning, illuminating pathways through the complex landscapes of risk, compliance, and transformative strategy.

Here, in this hallowed space, organizations do not simply adapt—they rise, they evolve, they conquer. The GRC Summit Egypt is a clarion call to the bold, the innovative, the unyielding: those who understand that in the face of constant change, true leadership is not about survival, but about defining the very future itself.


The GRC Summit Egypt
blends ancient wisdom with
cutting-edge innovation,
empowering leaders to ignite
transformation with agile
governance in a world of
constant change.

Ahmed El Shanet's Words

From Threat to Opportunity: How Cybersecurity Enhances Operational Efficiency

Cybersecurity plays a crucial role in enhancing operational efficiency by ensuring the smooth functioning of systems and protecting sensitive data. Here are some key ways in which cybersecurity contributes to operational efficiency:

Minimizing Downtime

- **Prevention of Cyberattacks:** Robust cybersecurity measures such as firewalls, intrusion detection systems, and regular updates help prevent cyberattacks that can lead to system failures and data breaches.
- **Quick Incident Response**: Effective incident response plans and tools allow organizations to quickly identify and address security threats, minimizing downtime and potential damage.

Protecting Critical Data

- **Data Loss Prevention:** Cybersecurity solutions safeguard sensitive data from unauthorized access, theft, or destruction, ensuring business continuity and regulatory compliance.
- **Data Backup and Recovery:** Regular data backups and disaster recovery plans enable organizations to quickly restore data in case of a data breach or system failure.


Chief Operating officer
Emirates NBD

Streamlining Operations

- **Automation of Security Tasks:** Automated security tools and processes reduce manual effort, freeing up IT staff to focus on strategic initiatives.
- **Improved Collaboration:** Secure collaboration tools enable efficient communication and teamwork, even for remote or geographically dispersed teams.

Building Trust and Reputation

- **Customer Confidence:** Strong cybersecurity practices demonstrate a commitment to protecting customer data, building trust and loyalty.
- **Regulatory Compliance:** Adherence to cybersecurity regulations helps avoid costly fines and legal issues, streamlining operations.

Cost Savings

- **Reduced Incident Response Costs:** Proactive cybersecurity measures can significantly reduce the costs associated with responding to data breaches and cyberattacks.
- **Improved Efficiency:** Streamlined operations and minimized downtime contribute to overall cost savings.

Competitive Advantage

- **Enhanced Customer Trust:** A strong cybersecurity posture can differentiate businesses and attract customers who value data privacy and security.
- **Faster Time to Market:** Efficient operations and minimal downtime allow businesses to bring products and services to market faster.

By investing in cybersecurity, organizations can create a more secure and efficient digital environment, ultimately driving business success.

Ahmed Abu el saad's Words

Africa's Financial Awakening: The Fintech Boom Redefining Access and Inclusion – EGYPT Case Study

Across Africa, a financial revolution is breaking down barriers, bringing essential services to millions through the rise of fintech. Driven by the need to overcome financial illiteracy and market volatility, the continent is transforming how financial services reach its diverse population. Africa's young, tech-savvy population—expected to make up over 60% of the continent by 2050—is fueling a strong demand for easy-to-access and adaptable financial services. Traditional banking has struggled to reach large segments of the population across Africa, leaving many without access to formal financial services. For Instance, in Sub-Saharan Africa, only 36% of adults possess basic financial knowledge, creating significant barriers to financial inclusion. This limited financial literacy, combined with ongoing economic instability, has posed serious challenges for the financial services industry in effectively extending its reach and supporting underserved communities.

Fintech has emerged as a solution to these challenges, offering digital platforms that provide services like banking, consumer finance, and investment. Since 2019, investment in African fintech has surged, with Nigeria, South Africa, and Egypt securing $2.7 billion, $1.7 billion, and $1.2 billion, respectively. These investments reflect confidence in fintech's potential to address Africa's unique needs.

Egypt has become a significant player in North Africa's fintech landscape. Driven by a young, digitally engaged population, Egypt's fintech sector is growing at an annual rate of 30%. Notable startups like MNT-Halan, which raised $815 million, highlight the industry's potential. Other companies, including Paymob and MoneyFellows, are advancing digital payment, credit, and savings solutions, making essential services more accessible to Egyptians.

A pivotal development occurred in 2024 when Egypt's Financial Regulatory Authority introduced a framework for fully licensed fintech operations. This shift led to Azimut Egypt's launch of "azinvest," the country's first licensed investment platform aiming to democratize investments, allowing Egyptians to invest directly from their phones and supporting Egypt's broader commitment to financial inclusion.

The impact of these initiatives is clear. In 2016, only 27% of adults in Egypt had access to financial services. By 2022, this rose to 64.8%, and by the end of 2023, it reached 70.7%, with 46.9 million financially included adults out of 66.4 million eligible individuals. This growth reflects the effectiveness of Egypt's fintech initiatives and regulatory reforms. Additionally, mobile payment transactions have surged, with values exceeding $3 billion and an expected annual growth rate of 18%, indicating a strong embrace of digital finance.

CEO
Azimut Investments

Egypt's fintech journey is part of a larger movement across Africa, where expanding connectivity is enabling fintech companies to tap into underserved markets. Egyptian fintech companies are not only meeting these needs but also enhancing financial literacy and access.

For other emerging markets, Egypt's path offers a powerful example of how agile governance and supportive regulations can enable fintech to address persistent challenges. Africa's fintech revolution signals a future where technology-driven finance empowers individuals, strengthens economies, and reshapes lives across the continent.

Maha Hasebou's Words

Are you ready for CBAM compliance?

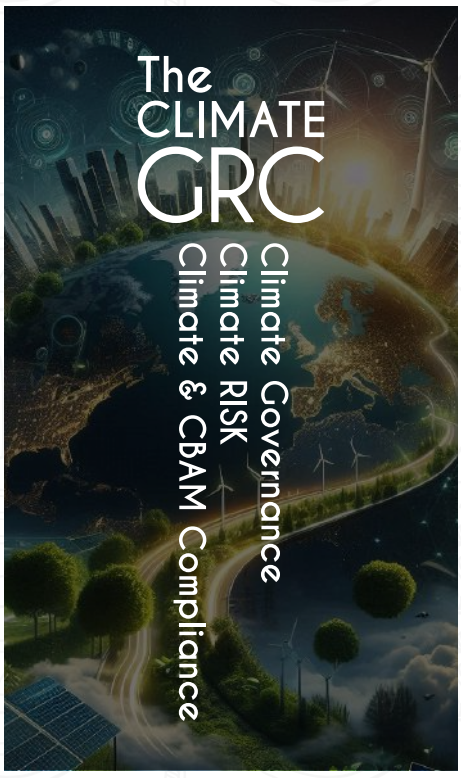
Dear Cement, iron, steel, aluminum, and fertilizers .. Business Owners, Importers and Traders,

If you are exporting to Europe, but not familiar with the European Green Deal? or CBAM? or Carbon Footprint? or Climate Risk? .. Then this article is for you.

Global Risk Report ranked Climate Change among the leading top 10 global risk within years. The Climate Change Performance Index (CCPI) indicates the EU is collectively responsible for 90% of the global GhG emissions (out of 63 countries index listed).

What is the European Green Deal ? On December 11, 2019, the Green Deal was officially launched by European Commission, to set Europe as the first climate-neutral continent in the world by 2050. This includes carbon taxation under the new compliance and regulatory law, Carbon Border Adjustment Mechanism "CBAM" specially on climate less ambitious countries . The European Green Deal tackles three key goals:

- **To Set Europe as the first climate-neutral (zero carbon) continent in the world by 2050 as a law;**
  1. In March 2020, the EU proposed the first EU Climate Law; to set legally binding EU climate targets.
  2. In 2021, the "Fit for 55 Packages" set GhG emission reduction targets 55% less by 2030 (vs. 1990); strengthen renewable energy target (currently 32%); and



set a higher price on CO2; while ensuring a fair competition for the European industry against peers.

3. On June 2023, the European Sustainability reporting Standards (ESRS) started requiring companies to disclose their ESG impacts.
4. In Feb. 2024 an additional target of 90% less emissions by 2040 was recommended.

- **Support a new EU industry Strategy: Sector integration strategy** (meaning how to electrify and decarbonize transport, heating and industry); and EU strategy for offshore wind (a new approach to grid connections, and to maritime spatial planning) and onshore wind; and strong focus on 2030 National Energy and Climate Plans.
- **A Sustainable Europe Investing Plan** worth €1 trillion to ensure a "Just Transition" - check Just Transition Fund and Social Climate Fund.
- **What is " CBAM"?**
  1. On 16 May 2023, the CBAM Regulation1 was published by the EU, which directly impacts energy-intensive industries by pricing the carbon emissions embedded in their products and to encourages industries worldwide to embrace greener production methods. CBAM seeks to impose a tax, if imported goods production had an emission higher than the EU's emission standards .
  2. Starting Jan. 2026, the EU plans to impose a 25% tariff on six key energy-intensive goods: iron & steel, cement,

fertilizers, aluminum, hydrogen and electricity.

3. CBAM Transitional phase (2023-2025) mandates industries on reporting carbon emissions for imported goods. Importers will be required to purchase CBAM certificates corresponding to their imported good emissions – as well as to avoid penalties -. This is considered a phase out of free allowances under the EU Emissions Trading System (ETS).

- **How will Egypt's Trade and Export be impacted by CBAM?**

Many countries are concerned about CBAM potential impact (risk) on their exports, and compliance level with the World Trade Organization (WTO). Egypt as a member of the WTO and a key exporter partner to Europe (21.7% are Egypt's export to Europe).. and could be impacted as follows:

1. **CBAM could disproportionately affect Egypt's exports of carbon-intensive goods like fertilizers:** In 2022, Egypt's exports of goods to the EU subject to CBAM – such as cement, fertilizers, and steel – were valued approximately at €4.6 billion (about 10% of the country's global exports); those highly energy-intensive and carbon-emitting industries are part of the manufacturing industry which accounts for 16% of Egypt's GDP. Manufacturers will pay for Carbon Credits and Certificates if the carbon emissions of their production line exceeds the EU new carbon standards.
2. **Compliance and reporting challenges: starting October 2023;** exporters are mandated to report their carbon emissions to EU importers. This necessitates investments in monitoring and reporting infrastructures (systems), which may be resource-intensive for Egyptian companies.
3. **Potential Economic Consequences:** CBAM could lead to increased costs for Egyptian exporters due to carbon levies imposed on carbon-intensive products, reducing Egypt good's competitiveness in the EU Market, potentially affecting export revenues and economic growth.

- **How should companies prepare for CBAM ?**

First, start calculating direct and indirect emissions, and report on IFRS S1, S2. For Fertilizers industry, I invite you to check Carbon Footprint Calculator (CFC) for fertilizers, a tool developed by the EU that is free and accessible for any company within the fertilizers industry to measure its carbon footprint (Link: Login | app calc fert). Also check: Carbon Border Adjustment Mechanism - European Commission; CBAM Factsheet_FERTILISERS copy, Carbon Border Adjustment Mechanism – European Commission. Secondly, Build your knowledge; attend workshop about CBAM's compliance requirements and implications by AHJ, and Federation of Egyptian Industries (FEI). Thirdly, explore green technologies within your lines of production:

1. **Leveraging EU Support:** the EU has proposed financial and investment support package worth €7.4 Billion for Egypt (2024-2027), for green and digital transition.
2. **Aligning with EU standards:** Adopting sustainable practices and aligning with EU environmental standards, such as, upgrading production processes, improving EE (Energy Efficiency), and reducing GhG emissions.
3. **Investment in Green Technologies:** Egyptian Companies are exploring green ammonia production, to align with global decarbonization trends. Promoting green hydrogen production and promoting investment in renewable electricity generation – such as the development of Mediterranean Hydrogen Partnership.

EMBRACE THE FUTURE SHAPE THE PRESENT

GRC SUMMIT EGYPT WHERE TRAILBLAZERS TRANSFORM CHALLENGES INTO OPPORTUNITIES

BE THE CHANGE DRIVE THE REVOLUTION

Step into a world where leaders turn vision into action, complexity into growth, and innovation into a legacy. The future favors those who act boldly and lead the transformation!

Press to Watch

Ayman Khalifa's Words

Importance of managing Climate Risk in financial institutions

Chief Risk Officer
Standard Chartered Bank Egypt

Defining the Risk

Climate Risk mainly stems from two types, namely physical risk and transition risk. Physical risk manifests in the form of extreme weather events including but not limited to drought, heat stress, increase in hurricanes and cyclonic activities, rise in sea level, and floods. This can have a direct impact on clients' cash flows by impact on their operating assets and/or disruption of the supply chain and/or inability of the workforce to physically perform the operations. Also, there is another risk on the collateral value of assets that are located in impacted geographies. On the other hand, Transition risk could stem from:

- change in regulations to the extent clients incur additional costs such as Carbon taxes.
- change in customer behavior.
- Increase in Energy price.
- Product substitution, and
- Ban on high emitting operations.

The impact on banks from both risks can include a-increase in non-performing loans and b-increase in capital re-directed to Credit provisioning.

Assessing the Risk

For the Corporate and Institutional portfolios, Financial Institutions can assess climate risk using 5 steps:

- Identifying risks and transition plans, this includes data gathering from client documents and client outreach. It is important at this stage to understand the level of client awareness of the risk and their readiness in terms of having a credible transition plan and allocated funding as deemed required to mitigate the risks.
- Analyzing the risk whereby a risk rating is assigned based on time horizon impact and mitigating factors. The higher the risk the more important it is to have a defined mitigation plan and timeline to reduce the risk to acceptable levels.
- Evaluate the Risk. At this stage, the financial impact is quantified in the financial analysis and factored in the Credit decisioning whereby the outcome would be approving the credit along with defined risk triggers, and early warning signals to monitor.
- Portfolio Management and monitoring where the Risk function can set Risk Appetite as well as monitoring plans for high Climate risk-rated clients.
- Controls and assurance which could include control sample testing and independent assurance that the process and controls are followed and are effective.

For the secured retail portfolio; risk assessment can be based on the impact of acute and chronic physical risk impacting physical collateral. This can focus on certain products such as property mortgages. Impact on collateral valuation could come from energy price increases, added regulations on buildings' energy efficiency, and retrofitting costs.
For an unsecured retail portfolio, physical risk could have second-order effects on customers' ability to repay their debt.

" Managing climate risk is no longer optional—it's essential. From physical risks like extreme weather to transition risks driven by regulation and market shifts, financial institutions must adapt. By assessing these risks and embedding them into credit decisions and portfolio strategies, we protect our future, foster resilience, and empower sustainable growth. "

Ahmed Farahat's Words

Internal Audit QA & Continuous Improvement

In today's ever-changing business environment, organizations face unprecedented challenges. To navigate these complexities, internal audit functions must embrace a commitment to quality assurance and continuous improvement.

Internal audit serves as a vital component of effective governance to provide an independent assessment on adequacy and effectiveness of risk management, control processes and governance of an organization. In an agile environment, where adaptability and responsiveness are paramount, internal auditors must not only assess compliance, but also enhance organizational resilience.

Quality Assurance (QA) in internal audit establishes the credibility and reliability of audit processes. Implementing robust QA frameworks ensures that audits are conducted in accordance with the Global Internal Audit Standards, which leads to consistent and reliable results. This trust is essential for stakeholders, as it reinforces the internal audit function's role in safeguarding organizational integrity. To achieve a high level of QA, internal audit teams should:

- Align with the established standards to enhance the professionalism and effectiveness of audit activities.
- Undergo ongoing supervision and periodic assessments of audit processes and outcomes to help identify areas for improvement to ensure that the function remains relevant and effective.
- Encourage a mindset focused on quality across the organization that fosters collaboration and supports the continuous improvement attitude.

Continuous improvement is essential for internal audit functions to help achieve the organization's strategic objectives and remain relevant in a world characterized by constant change. The ability to adapt and evolve is crucial for responding to emerging risks, regulatory changes, and technological advancements. To facilitate continuous improvement, organizations should:

- Embrace data analytics and automation to enhance audit efficiency and effectiveness, allowing auditors to focus on high-risk areas and strategic insights.
- Invest in professional development to ensure that auditors are equipped with the latest skills and knowledge, enabling them to tackle complex challenges.
- Gather input from stakeholders to helps improve audit processes and enhances the value delivered by the internal audit function.

The integration of quality assurance and continuous improvement creates a dynamic feedback loop. A strong QA framework provides the foundation for identifying improvement opportunities, while continuous improvement initiatives enhance the quality of audit processes. This synergy positions internal audit as a proactive business partner in governance, risk management, and strategic decision-making.

In a world of constant change, internal auditors can contribute significantly to the success of an organization by positioning it to seize new opportunities and fostering a culture of trust, adaptability, and excellence through effective quality assurance and a commitment to continuous improvement.

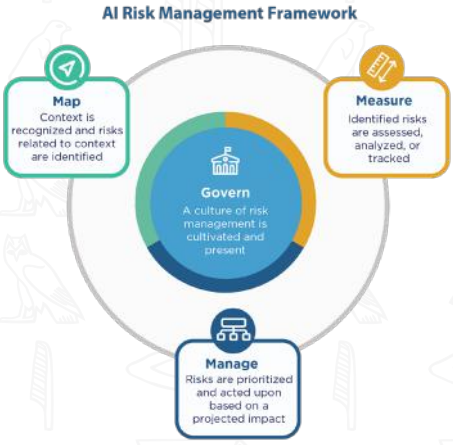
Waleed Soliman's Words

Cybersecurity Unveiled: Navigating the Risks Ahead of AI

Cybersecurity is a key factor in the competition for Artificial Intelligence dominance. Using AI technology to improve cyber defense capabilities can counteract the adverse effects of cyberattacks.
Organizations are quickly diving into the world of AI to improve their operations and obtain a competitive advantage. But it's important to realize that the journey with AI won't always be that smooth and easy.
As a business owner, you must understand that AI has many advantages, but it also has certain common challenges that arise when you integrate new technology into your daily operations.

Recognizing AI's Risks:

NIST's AI RMF 1.0, states that AI risks include possible risks to people, organizations, or systems as a result of creating and using AI systems.



Identifying the AI Challenges and Solutions:

Understanding and addressing these challenges at the appropriate time are essential to ensuring responsible AI adoption.


Deputy General Manager for Cybersecurity Risk & Resilience Central Bank of Egypt

Below some examples of AI challenges and solutions:

- **Privacy Challenges:**
  A threat to privacy is one of the biggest challenges facing AI. AI often needs to gather and examine enormous volumes of personal data, which raises privacy and security issues. Organizations must put data protection first by using data encryption methods, putting strong cybersecurity safeguards in place, and abiding by stringent privacy regulations. This can support preserving trust and protecting user privacy.
- **Security Challenges:**
  Security threats increase with the development of AI technologies. Malicious activity poses a serious risk to enterprises by taking advantage of AI systems and generating higher-risk attacks. Strong security measures, and AI-driven threat detection systems, should be put in place by organizations to reduce security threats. For the deployment of AI systems to be secure, constant monitoring and frequent vulnerability assessments are essential.
- **Legal and Regulatory Challenges**
  Liability and intellectual property rights concerns are among the new regulatory challenges brought about by AI. For legal frameworks to keep up with technological innovations they must change. Organizations may quickly evaluate large volumes of data and information while seeing potential issues related to compliance by using AI for risk and complaint solutions.

CONCLUSION

Although AI has many potential benefits for organizations, it presents many challenges. That is to say, the uncontrolled use of AI could have negative consequences. To overcome these obstacles and ensure that the technology improves organizations while reducing potential threats, the development and use of AI must be approached properly and ethically. This needs to be achieved by implementing education and awareness campaigns. This will ensure that the organization benefits from AI while minimizing risks and maximizing its potential.

Ioannis Kanaris's Words

How Analytics and Artificial Intelligence Are Revolutionizing the GRC Landscape

In today's rapidly evolving digital world, we're witnessing a significant transformation in how organizations approach GRC. Analytics and AI are no longer just buzzwords; they're becoming indispensable tools that empower us to navigate complex regulatory environments, mitigate risks, and make more informed decisions.
Embracing AI to Streamline GRC Processes.
Have you ever felt overwhelmed by the sheer volume of data and repetitive tasks involved in compliance? AI offers a solution. By automating routine processes, machine learning algorithms can sift through vast amounts of data to identify patterns and anomalies that might signal potential compliance issues or risks. This automation frees up our compliance teams to focus on strategic initiatives rather than getting bogged down in mundane tasks.

- **Making Smarter Decisions with Predictive Analytics:** Imagine being able to anticipate future risks before they become actual problems. AI-powered predictions, allow us with proactively addressing these risks, so we can implement measures to prevent them from escalating—a crucial capability in today's dynamic regulatory landscape where new compliance requirements emerge rapidly.
- **Enhancing Risk Identification and Compliance Monitoring:** With AI-driven analytics, we can now monitor compliance status and risk exposure in real-time. Technologies like Large Language Models enable us to analyze unstructured data—such as emails, documents even images and videos—to detect compliance violations that might otherwise go unnoticed. This heightened level of scrutiny ensures continuous compliance and reduces the likelihood of costly penalties.

Navigating Challenges and Ethical Considerations

While the benefits are significant, it's important for us to be mindful of the challenges AI presents. Handling sensitive information raises data privacy concerns, and biases embedded within AI algorithms can affect decision-making processes. Transparency is key; we must ensure that our AI systems are explainable and adhere to data protection regulations.

Integrating AI into GRC Strategies

So, how do we effectively integrate AI into our GRC strategies? Here are some guidelines that I consider to be useful:

- **Invest in Training:** Equip our teams with the skills to work effectively alongside AI technologies.
- **Continuous Monitoring:** Regularly assess AI performance and make necessary adjustments to address any issues.

Looking Ahead to the Future

As we move forward, AI's role in GRC is set to expand


CEO and Founder
DIGIAI

even further. Advanced AI models will provide deeper insights into risk prediction and compliance management. However, it's crucial that we balance technological advancements with ethical considerations. Staying informed about evolving regulations governing AI usage will help ensure that our adoption of these technologies remains compliant and responsible.

Conclusion

Analytics and AI are revolutionizing the GRC landscape, and together, we can harness these tools to enhance efficiency, improve risk management, and ensure compliance. By embracing these technologies responsibly and thoughtfully integrating them into our strategies, we can transform data into decisive action.

Navigating the Future:

The Intersection of Digital Governance, Innovation, and Sustainability

At the core of digital governance lies a vision where digital Governance, seamlessly integrate with innovation, sustainability, and digital transformation. This approach highlights the importance of adaptive leadership and agile governance in helping organizations navigate an ever-changing world. With sustainability at the forefront, renewable energy initiatives and global climate actions are paving the way for a greener future.

As technology reshapes industries, the impact of AI on governance, risk management, and compliance is becoming increasingly evident, while cybersecurity remains essential in protecting the digital landscape. The rise of fintech and a focus on arbitration and advanced risk management demonstrate how legal and financial systems are evolving to support global resilience.

Data privacy, identity management, and sustainable digitalization lie at the heart of responsible innovation. As GRC principles continue to guide organizational success, they also strengthen economic resilience, enabling businesses to adapt, innovate, and lead in today's fast-paced environment. This vision represents the fusion of traditional wisdom and cutting-edge technology, charting a path toward a sustainable and transformative future.

Kamal Fayek's Words

"Building a Future - Ready Internal Audit Function: Integrating New Standards and Frameworks for Enhanced Governance"

Head of Audit Quality Assurance & Follow-up
Banque Misr

In today's rapidly evolving business environment, organizations face increasing complexities that require a robust internal audit function. A future-ready internal audit is not just a compliance tool but a strategic partner in governance, risk management, and organizational performance.

The New Global Internal Audit Standards, developed by the Institute of Internal Auditors (IIA), provide a framework that strengthens internal audit functions worldwide. Organized into 5 domains, the Standards focus on key areas that ensure internal audits are effective and aligned with organizational goals. At the heart of the Standards are 15 guiding principles that enable successful internal auditing, supported by specific requirements, implementation considerations & evidence of conformance.

- **Domain I** "Purpose of Internal Auditing" helps internal auditors and stakeholders understand and articulate the value of internal auditing, emphasizing its role in supporting governance and risk management.

- **Domain II** "Ethics and Professionalism" replacing the IIA's former Code of Ethics & outlines the behavioral expectations for auditors, including Chief Audit Executives (CAEs) and staff as well as it fosters a culture of professionalism, integrity, and ethical behavior.

- **Domain III** "Governing the Internal Audit Function" focuses on the CAE's role in collaborating with the board to establish, position, and oversee the internal audit function's independence and performance. It also outlines a solution on how to deal with disagreements between CAE, the Board or Senior Management by displaying possible 14 questions the CAE may get along with potential responses.

- **Domain IV** "Managing the Internal Audit Function", the CAE is responsible for managing according to the internal audit charter and Global Internal Audit Standards. This includes strategic planning, resource management, stakeholder communication, and enhancing audit performance to ensure the function aligns with organizational objectives.

- **Domain V** "Performing Internal Audit Services" outlines how auditors should plan and conduct audits, develop findings and conclusions, collaborate with management on recommendations, and communicate effectively throughout the audit process.

Finally, building a future-ready internal audit function requires a proactive approach that incorporates new standards and frameworks, leverages technology, and encourages continuous learning. By adopting these changes, organizations can ensure their internal audit functions do more than just meet compliance requirements. They can become essential partners in driving governance, risk management, and strategic decision-making. This shift will position internal auditors as key contributors to organizational success in a complex, fast-changing business environment.

Sherif Ata, 's Words

Leveraging emerging technologies for Internal Audit Efficiency

In today's fast-evolving and demanding business environments, internal audit functions are actively exploring emerging technologies to enhance their efficiency, effectiveness, and value-addition. By embracing innovative tools and methodologies as follows:

- **Data Analytics and Artificial Intelligence;** One of the most significant advancements in internal audit practices is the incorporation of data analytics and artificial intelligence (AI). These technologies have dramatically transformed the way auditors process and analyze vast volumes of financial data. AI algorithms can now detect anomalies, trends, and patterns in data, making it easier to identify potential irregularities or fraud incidents.
- **Continuous Auditing and Monitoring (CAM);** The intro of CAM has transformed the traditional periodic assessment approach to a real-time, ongoing evaluation of an organization's processes and transactions. This continuous approach allows auditors to detect and address issues promptly, enabling organizations to mitigate risks and improve their overall control environment. By leveraging CAM, internal auditors can provide timely insights to management, identify and address control weaknesses more quickly, and enhance the organization's ability to respond to emerging risks
- **Robotic Process Automation (RPA);** Robotic Process Automation has emerged as a powerful tool for internal auditors to automate repetitive and rule-based tasks. By implementing RPA, internal auditors can streamline audit processes, optimize audit procedures, and focus on more strategic and value-added activities.

Challenges and Considerations

While emerging technologies bring significant benefits for internal audit efficiency, its implementation comes with challenges:

- **Skill Development:** As technology advances, auditors need to continually self-develop their skills to stay adept in their field. This includes learning to use new audit software and understanding the implications of emerging technologies.
- **Data Privacy and Security:** With the increased use of technology, auditors must adhere to data protection regulations, especially when dealing with sensitive financial information. Compliance with data privacy laws is essential.
- **Integration and Implementation:** Adopting new technologies may require significant changes to existing audit processes and systems. Organizations need to carefully plan and manage the integration of these technologies to ensure smooth implementation and maximize their benefits and efficiency.
- **While consideration for Adoption of digital technologies can have two kinds of outcomes:** optimizing existing processes or transforming processes and methodologies by introducing new techniques and approaches. Both are valid, worthwhile outcomes, but clarity and awareness on the purpose of introducing new technologies are essential.

Conclusion

By leveraging data analytics, AI, continuous auditing and RPA, internal auditors can transform their role from mere assurance providers to strategic partners and advisors in their organizations' pursuit of effective risk management, operational excellence and effective governance. As these technologies continue to evolve, it will enable more robust, efficient, and effective audits. Internal audit functions must embrace these innovations while carefully navigating the associated challenges and opportunities to deliver enhanced value to their organizations.

Mahmoud Elbagoury's Words

Detect, Deter & Prevent: Integrating Anti-Fraud Initiatives into Your Risk Management Program

In today's fast-paced, ever-changing global environment, organizations face a multitude of risks. the threat of fraud is ever-present and increasingly sophisticated. Integrating anti-fraud initiatives into your risk management program is not just a necessity but a strategic imperative. As organizations strive to adapt to the future, guided by the principles of agile governance, a proactive approach to fraud management is essential to navigating the complexities of a constantly changing world

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

Detect: Harnessing Technology and Data Analytics

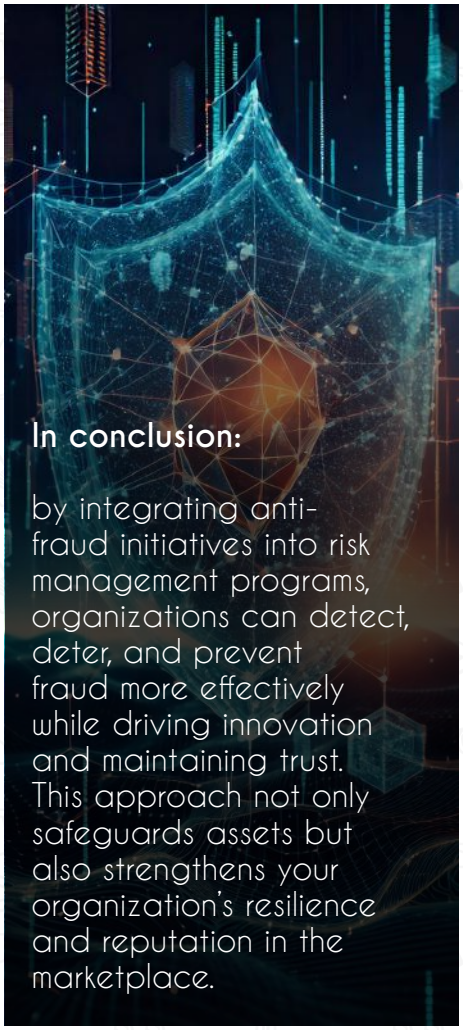
The first step in combatting fraud is early detection. Modern organizations have access to vast amounts of data, which, when leveraged effectively, can uncover fraudulent activities early. Advanced technologies like artificial intelligence (AI) and machine learning (ML) empower organizations to analyze patterns, identify anomalies, and flag potential fraud indicators in real-time, identify irregularities early and respond swiftly.
Key practices in fraud detection: Continuous Monitoring, Regular Audits, Predictive Analytics, Data Analytics and AI, and Reporting Channels

Deter: Creating a Fraud-Resistant Culture

Deterrence is about making fraud too risky or unappealing to attempt. Detection alone is insufficient; organizations must actively deter fraudulent behavior by fostering an environment where fraud cannot thrive. Deterrence relies on transparency, accountability, and a culture of integrity.
Effective deterrence strategies include: Tone from the Top, Establishing Clear Policies, Strengthening Internal Controls, Training and Awareness Programs, and Promoting Transparency.

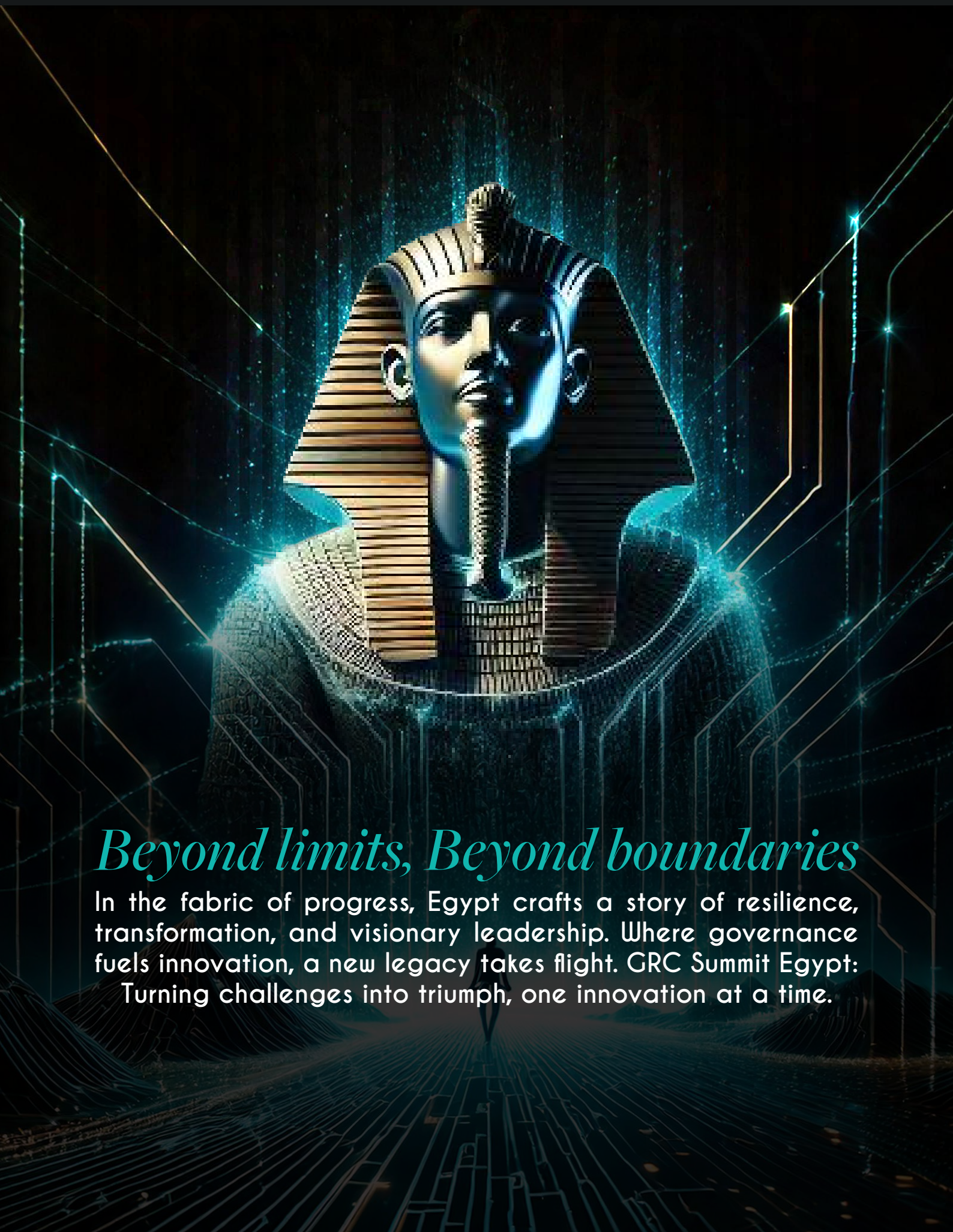
Prevent: Building Resilience into Processes

Prevention is the ultimate goal of any anti-fraud initiative, and it begins with designing systems that make fraud difficult, if not impossible. Prevention also means embedding fraud-resistant processes into the organization's DNA.
By embedding fraud risk management into core processes and decision-making, organizations can minimize vulnerabilities.
Preventative measures should involve: Integrating Fraud Risk Assessments, Leveraging Agile Frameworks, Fostering Collaboration, Integrated-Risk Management Tools, Cybersecurity Measures, Third-Party Due Diligence, Employee Background Checks.



In conclusion:

by integrating anti-fraud initiatives into risk management programs, organizations can detect, deter, and prevent fraud more effectively while driving innovation and maintaining trust. This approach not only safeguards assets but also strengthens your organization's resilience and reputation in the marketplace.



Beyond limits, Beyond boundaries

In the fabric of progress, Egypt crafts a story of resilience, transformation, and visionary leadership. Where governance fuels innovation, a new legacy takes flight. GRC Summit Egypt: Turning challenges into triumph, one innovation at a time.

Ramzy El Masry's Words

A Historical Landmark Year for Regulations

The rapid evolution of the digital landscape, exemplified by the 2023 launch of ChatGPT,which took the world by surprise and caused a paradigm shift in AI applications, this was paralleled by a surge in digital regulations. The EU's "A Europe Fit for the Digital Age" priority as part of the 2019-2024 strategy has driven the development of numerous directives and acts. While some of these regulations were enacted in 2022, their full effects, including enforcement mechanisms, only came into force in 2024 after the conclusion of transitional periods. This recent wave of regulatory activity, particularly the EU Commission's focus on digital trade, has once again caught the world by surprise.

Before we dive into those developments and their relevance to everyone outside the EU, it's important to understand the difference between a regulation, an act and a directive, to make sure we understand the consequences of each on compliance.

A "Regulation" is a binding legislative act. It must be applied in its entirety across the EU, and the same applies for an "Act" that is also binding and applied in its entirety across the EU, while a "Directive" is a legislative act that sets out a goal that EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals , from these definitions we can already know that a directive is going to be harder to adhere to, since it requires from the enterprise to see which individual(s) law within which EU member state that will apply for it.

Nov 2022, the Digital Market Act (DMA) enters into force, this regulation 'establishes a set of clearly defined objective criteria to qualify a large online platform as a "gatekeeper" and ensures that they behave in a fair way online and leave room for contestability', the objective of this regulation is to make sure large companies deemed as "Gatekeepers" can't deny a smaller market player entry into the market, making sure innovators and startups have a fair entry into the market and also from consumers perspective they are saved from monopoly strategies.

Those "Gatekeepers" are basically defined as 'are large digital platforms providing any of a pre-defined set of digital services ('core platform services'), such as online search engines, app stores, and messenger services',

This regulation became applicable in 2nd May 2023 but it wasn't until march 2024 the full application of obligations came to force, a glance of those Gatekeepers can be seen below

Figure from official website of EU[2]

Same Month Nov 2022, Digital Services Act (DSA) enters into force as it 'regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. Its main goal is to prevent illegal and harmful activities online and the spread of disinformation', mainly targeting Very Large Online Platforms (VLOPs) as well as Very Large online search engines (VLOSEs) for stricter rules but others are also targeted with this regulation such as Online platforms and Hosting services and intermediary services

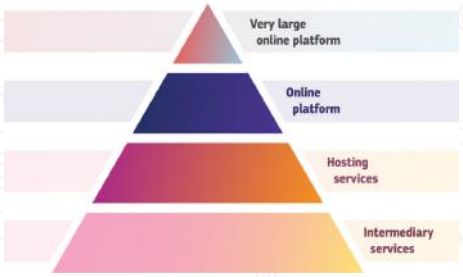


Figure from official website of EU[3]

August 2023, rules of this regulation applied for VLOPs/ VLOSEs and as of Feb 2024, it applied to all other platforms.

One would see clearly that the EU took a top-down approach for both the DMA & DSA regulation by targeting stricter rules for larger companies, while not discarding the fact that ISPs, DNS registrars/providers and Cloud as well as web-hosting providers of all sizes are under the DSA, and thus year 2024 is monumental as smaller companies across EU have to adhere to those rules too, Basically resulting of more transparency requirements, more independent oversight, which results in increased need for more Compliance Officers & Internal auditors to understand the regulations to be able to comply and/ or audit those Acts, Providing the independent oversight committees set by the EU or delegated to local governments across the EU member states proper & timely reporting, Noticeably in most of those acts if a company is located outside the EU but has a representer within EU, like for example an importer, they bare the responsibility to be compliant.

In 2018, GDPR came into force causing loads of impact, and entities within the EU and outside, had to comply with it, even inspiring other jurisdictions outside the EU to create their own Data Protection laws, January 2024, the "Data Act" entered into force, with full effects to be seen September 2025, this regulation 'is a comprehensive initiative to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data' and along with the "Data Governance Act", which 'seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.' & 'support the setup and development of Common European Data Spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.' which came into effect Sept 2023. Those two came to amend GDPR and regulate/introduce transparency along the "Data Economy", in terms of monetizing the data sharing and/or making it more safe to.

Following the regulation of Digital Markets & Services Acts , which is seen as infrastructure of the Digital Economy, and the amendment of the GDPR by the Data Governance Act (DGA) and the Data Act, as pillars for Data Economy, the EU wanted to go towards both the Public and Private Sector and address the obvious requirements which are the Digital Products themselves and their supporting infrastructure plus the trending development.

And thus We had 3 developments, 2 regulations and 1 directive. We start with the directive since it's an upgrade of the Network & Information Security (NIS) 2016 . NIS2 was approved in 2022 and came into effect in Jan 2023 with transition to till Oct 2024, for all the EU member states to adopt the directive into national laws, and the importance of that directive is the fact that all private and public entities are differentiated via Size and Sector, into multiple categories, each of which has a proportional set of requirements, which are almost ISO 27001:2002 like and/or Equivalent, and what is very important to mention about it, is that an Software-as-a-Service (SaaS) provider will become regulated under NIS2, while this leads us to also talk about the "Cyber resilience act (CRA)" is focusing on Software and products (physical) that has a digital aspect, and affect quite well the support models and their documentation and obligations towards the manufacturer.

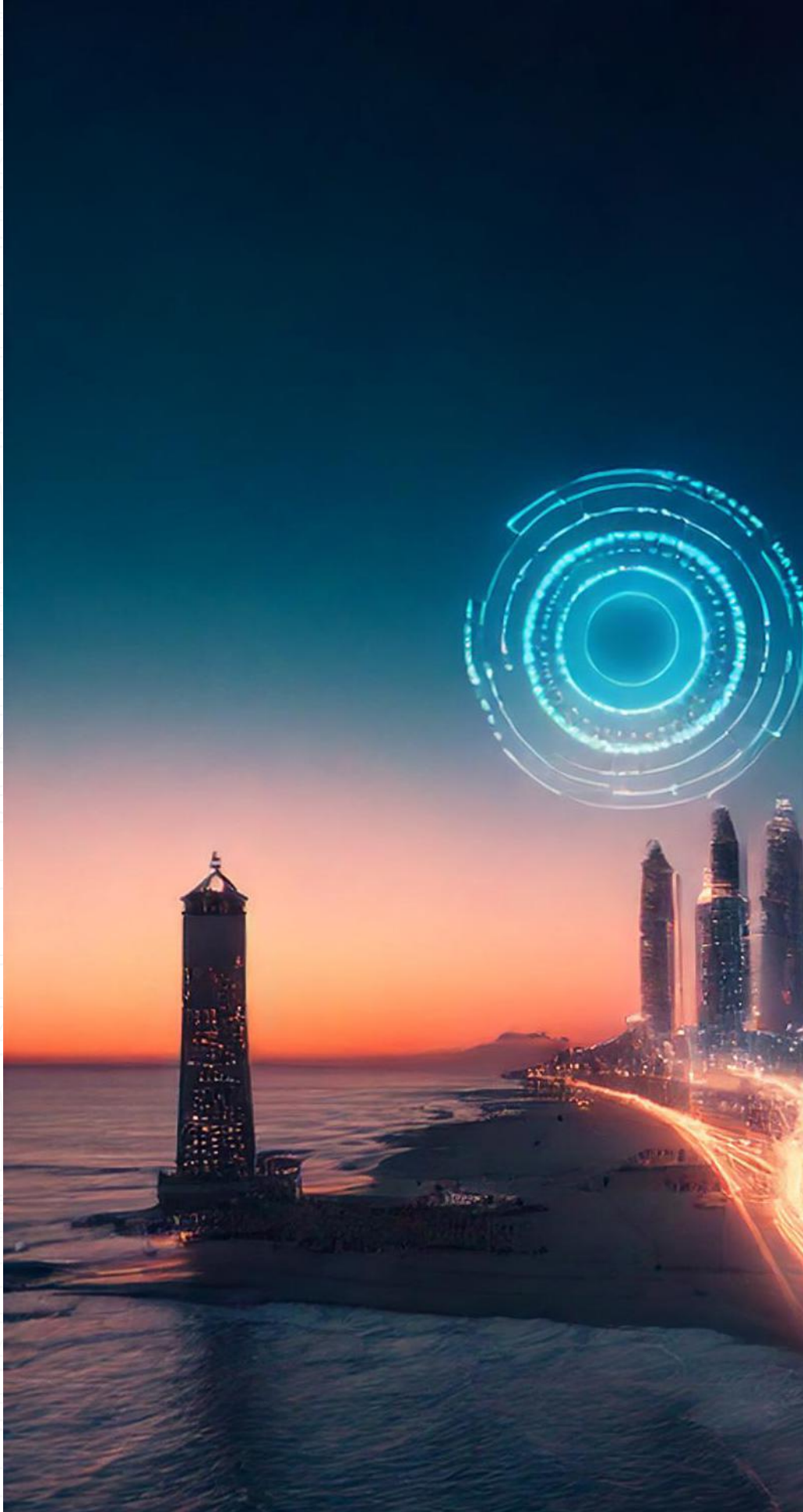
On a different angle, the "Artificial Intelligence act(AI Act)" was approved in June 2024, and it's the first Artificial Intelligence legislation to formulate different requirements according to the risk level imposed by the application of the AI itself, it is important to notice, that a lot of people identify AI with Generative AI, or ChatGPT as an application, while the AI Act is defining this as "AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;' which as clearly stated, could also

mean a Machine Learning (ML) algorithm used for example for fraud detection and/or decision making, this will have a wide implications, when it becomes fully effective as an act in August 2026, but the first actual requirement for compliance is as close as Feb 2025, so few months ahead.

Looking back on all the regulations provided within this article, one would have a couple of questions to ask
1- Which regulations affect the business I am representing ? or since i am outside the EU i am not affected ?
2- Am I ready as a Professional for all the requirements in those laws ?

The answer for the first question is simple, if you want to do business with the EU, then you will have to accept to be regulated with EU laws, and thus you need to be compliant.

The answer for the second question is harder to answer, and i would leave it to the reader to add to my humble answer,
"We need a unified compliance platform, in which you create an internal framework with the objective of test once comply many, but also, you need to utilize multi-disciplinary teams to achieve compliance, few years ago we said , Security Shift-Left, meaning that we want to include some of the security responsibilities into operations, is it time to say Compliance Shift-left ?"



1. A complete definition could be found at https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en
2. The Gatekeepers list https://digital-markets-act.ec.europa.eu/gatekeepers_en
3. The full definition of the providers covered https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
4. NIS 1 - URL - https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148
5. NIS 2 - URL - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227
6. CRA - URL - https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html
7. AI ACT - URL - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

From Pyramids to Pixels:

Shaping the Future of Digital Governance

Where ancient pyramids meet the forefront of digital governance, we come together—not just as leaders, but as architects of tomorrow's governance.

Our ancestors built civilizations from stone and sand; now, we shape the future with data, vision, and unstoppable courage.

This isn't just a summit—it's a revolution. Every protocol is a bold step forward. Every strategy, a tool for transformation. Every leader, a pioneer reshaping the digital age.

At GRC Summit Egypt, uncertainty bows to innovation. We don't just manage systems—we reinvent them.

Ignite change. Lead boldly. Embrace the future.

The revolution *Begins* now.

Introduction

A strong Governance, Risk, and Compliance (GRC) program is essential for sustainable growth and resilience. It helps manage risks, promotes ethical behavior, and ensures regulatory compliance. However, implementing GRC can be challenging due to limited awareness and resources, but the right tools and strategies can make it successful.

An effective GRC framework supports decision-making, streamlines compliance, and improves resilience. Additionally, by using structured policies, technology, and involving key stakeholders, organizations can create a sustainable GRC program that enhances business integrity and performance.

Furthermore, a detailed roadmap helps align GRC with strategic goals and fosters accountability and transparency.

Roadmap for Establishing a GRC Program

- **Understand Current Practices:** Assess existing governance, risk management, and compliance (GRC) practices.
- **Define Vision and Objectives:** Articulate a clear vision for the GRC program. Set specific, measurable, achievable, relevant, and time-bound (SMART) objectives that align with the organization's strategic goals.

Sami Ben Jouda's Words

Enterprise GRC by Design: Blueprint for an Effective, Efficient & Agile Enterprise GRC Management Program

- **Clarify Roles and Responsibilities:** Define the roles of key stakeholders such as the board, senior management, risk officers and compliance teams, must understand their role in GRC, ensuring accountability and ownership.
- **Form a GRC Steering Committee:** Establish a team from key departments for oversight.
- Create a GRC Department: Centralize GRC management with clear roles and qualified professionals.
- **Develop a GRC Framework:** Outline policies, procedures, and processes.
- **Manage Policies and Procedures:** Standardize and regularly update to ensure compliance.
- **Establish Communication Channels:** ensure that risk and compliance issues are promptly identified and addressed. Additionally, creating mechanisms for reporting and escalating issues to senior management and the board of directors is essential to ensure timely and effective resolution.
- **Implement GRC Tools:** Use technology for better data visibility and risk management.


General Manager
GRCA Solutions & Consulting

- **Conduct Comprehensive Risk Assessment:** conduct risk assessment to identify and assess known and emerging risks. Developing a risk appetite statement helps define the boundaries within which the organization operates, guide decision-making, and prioritize risk responses based on strategic objectives.
- **Address Data Privacy and Cybersecurity:** Implement measures to protect sensitive information.
- **Implement Training Programs:** Raise awareness and foster a compliance culture.

- **Monitor and Review Performance:** Continuously improve the GRC program using feedback and audits.

By following these steps, organizations can develop a resilient GRC program that enhances business performance and sustainability.

Essential Tools for Effective GRC Implementation

- **Three Lines of Defense Model:**

By implementing the Three Lines of Defense Model, organizations can create a structured and robust approach to governance, risk management, and compliance. This model helps to clearly define roles and responsibilities, enhance communication and coordination, and ensure that risks are managed effectively across the organization.

1. **First Line (Operational Management):** Managers and employees manage risks daily, implementing controls and ensuring compliance.
2. **Second Line (Risk Management and Compliance):** Specialized teams develop and monitor compliance programs, supporting the first line.
3. **Third Line (Internal Audit):** Internal auditors provide independent assurance, evaluating the effectiveness of the first two lines.

COSO Internal Control Framework:

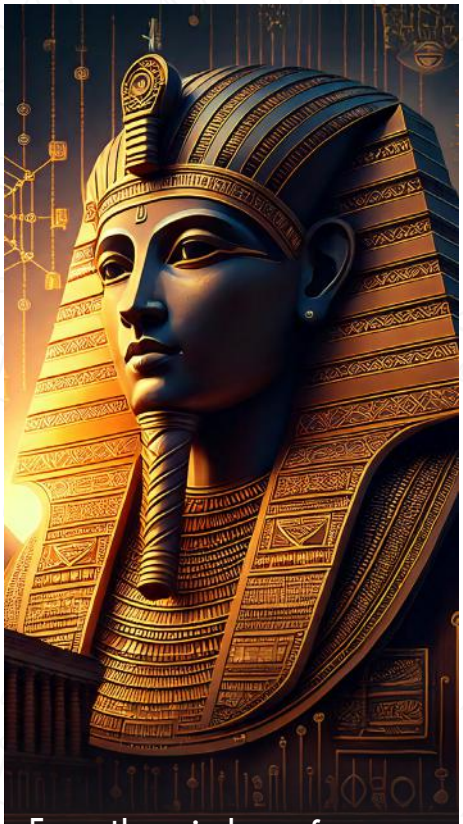
Adopting the COSO Internal Control Framework, established by the Committee of Sponsoring Organizations of the Treadway Commission in 2013, can be an exceptionally effective strategy for implementing a GRC program. The framework covers five interrelated components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.

1. **Control Environment:** Promotes ethical conduct, integrity, and accountability.
2. **Risk Assessment:** Aligns with Enterprise Risk Management (ERM) to identify, analyze, and prioritize risks.
3. **Control Activities:** Procedures to ensure compliance and manage risks.
4. **Information and Communication:** Ensures timely and accurate reporting.
5. **Monitoring Activities:** Continuous evaluations to improve governance, risk management, and compliance processes.

By using COSO model, organizations can enhance their GRC programs, ensuring accountability, transparency, and effective governance.

Conclusion

In conclusion, developing a successful Enterprise GRC management program requires a strategic approach that seamlessly integrates governance, risk management, and compliance into a cohesive framework. By concentrating on key components, such as corporate objectives and strategies, executive sponsorship, stakeholder alignment, comprehensive risk assessments, policies and procedures governance, robust policy management, advanced technology integration, decision-making, transparency, responsibility, and accountability, organizations can establish a GRC program that effectively supports proactive risk management and regulatory compliance. Ultimately, a meticulously crafted GRC program serves as a foundational pillar for securing long-term organizational success.



From the wisdom of ancient to the precision of modern algorithms, the GRC Summit Egypt bridges heritage and innovation, crafting a future where digital governance upholds the legacy of integrity and resilience.