WHITE PAPER

TRANSFORMING GRC FOR THE DIGITAL ERA

Infosys®
Navigate your next

Governance, Risk and Compliance (GRC) refers to an organization's coordinated strategy for managing the wide issues of corporate governance, enterprise risk management (ERM) and corporate compliance w.r.t. the regulatory requirements. As per Open Compliance and Ethics Group (OCEG), GRC is defined as a system of people, processes & technology that allows an organization to: a) understand & prioritize the stakeholder expectations; b) set business objectives which are consistent with the firm's values & risks; c) achieve these objectives while optimizing the risk profile & protecting value; d) operate within legal, internal, contractual, ethical & social boundaries; e) provide reliable, relevant, and timely info to the appropriate stakeholders; and f) enable the measurement of performance & effectiveness of the firm's system.

In the past, GRC was only seen as a set of business functions, capabilities, and processes for meeting the defined organizational objectives and report lapses, if any. Also, in the past, risk types were limited and could be tracked using simple tools and methodology.

However today, as we know, businesses are opening-up to newer and sophisticated technologies and channels — as a move towards the 'Digital Era'. Consequently, over the past few years, the scope of risks within the purview of GRC has increased manifold. Today, businesses are encountering greater uncertainty in a wide array of new and emerging risks. The ever-evolving globalization of competitive markets have exposed organizations to new breed of risks. Organizations have been unable to anticipate and plan for these new breed of risks — such as cyber-attacks, cloud security, competitor shifts, climate change and geopolitical crisis.

Given the turbulent ecosystem, organizations need to rapidly revamp and re-architect their GRC solutions so as to expand their risks coverage and be better prepared for the future changes. To aid this transformation, in this paper, we suggest certain pillars that, in our view, need to be an integral component of any GRC transformation. We also illustrate few examples of efficient GRC practices.

Governing Principles: Pathways to advance towards Digital GRC

- **Empowered individuals & people centric approach:** Organizations should cut the red tape and enable managers/ tower-owners to take decisions. Further they should provide staff with an opportunity to be part of the GRC framework; and enable means for their active participation. The GRC framework should empower individuals to voice their views, and inform about the potential breaches, incidents and system loopholes that they come across.
- **Ability to absorb and ingest grassroots information:** The future of any organization largely depends on its ability to proactively read the external and internal indicators and take timely action. Hence, it is important that organizations' GRC functions are designed in a way that these can take inputs from various sources, ingest it and then report back as meaningful metrics that can aid in accurate and informed decision making.
- **Cutting-edge technology:** Today, web technology has become a key enabler for businesses to support and implement complex GRC. Therefore, it is important that the organization's technology footprint become capable of mobilizing, digitalizing and optimizing all of the firm's risk and compliance related activities. Further, this technology capability needs to be embedded across the organization, and should be able to engage all stakeholders as per their individual needs. This is a key pillar of GRC transformation, as all of the other pillars would need technology aid to fully scale-up and perform to the desired level.

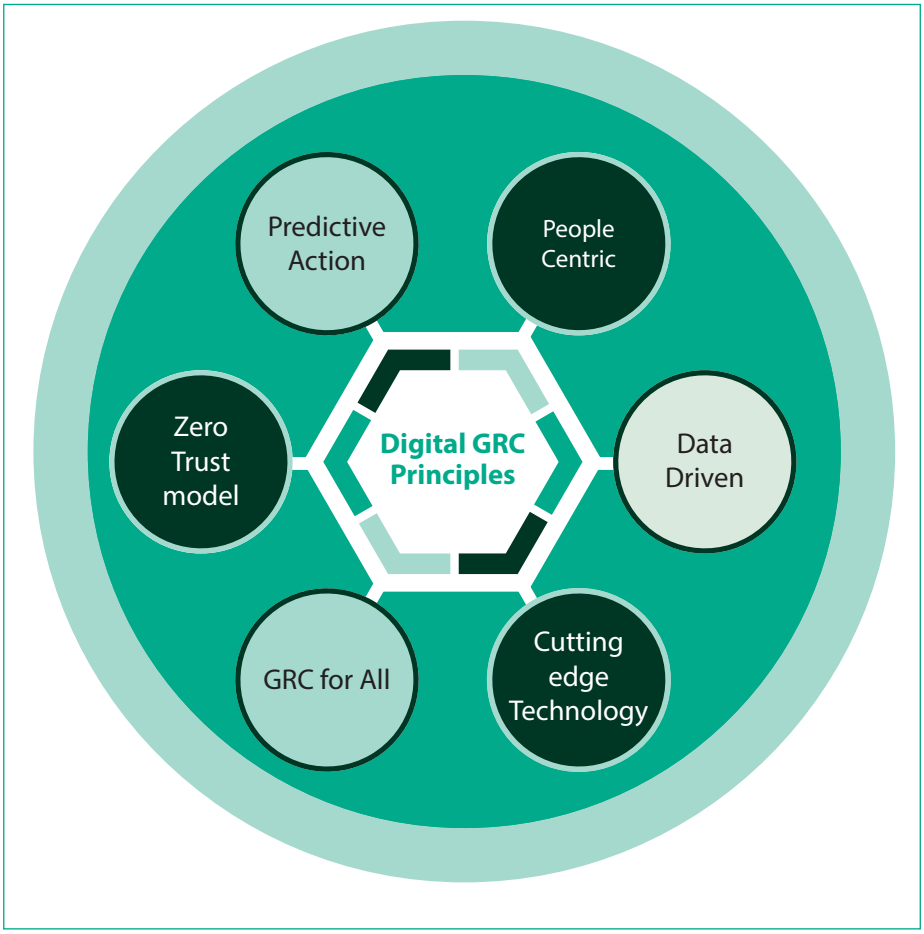

Exhibit 1 – Key Digital GRC principles

- **"GRC for All":** Firms should enable employees at all levels to participate in the GRC process — rather than solely reserving it for those who have access to the GRC system or apps. Capability should be built to report, investigate and track incidents across employee levels. This will ensure that the risk perimeter covers all - and means are created to report and track even the smallest of incidents.
- **Embracing the "Zero Trust" model:** Given the increased risks, organizations should do away with their current compliance approach that is based on sample verification. This should be replaced by a holistic approach that tests all of the controls so as to provide a truly compliant view. Testing with samples leaves high chance of default - more so now when the effect of the sample data is multiplied with the diverse risk types.
- **Move towards real-time analysis:** Organizations need to shift away from their current approach of reactively analyzing the past incidents and then putting in controls once the transaction has already occurred. In its place, the firms' new GRC capabilities should enable enhanced controls — that provide the ability to stop or terminate an erroneous transaction or process on the go and before it happens. To enable this transition, firms need to carefully study their controls and systems, prioritize and then decide upon the ones that need to be enhanced. This is because all such enhancements and interventions have significant cost implications for the firm.

Translating the Governing Principles to ground action: Few examples and recommendations from Infosys

For GRC frameworks and programs to be truly effective, organizations need to work with a 360-degree view of their compliance to policies. This will help ensure that the GRC processes are developed and applied consistently across the enterprise. Making this happen require that not just the connected business applications and processes, but also the core GRC activities of the organization are enhanced/added in alignment with the key digital trends, the systematic changes inside and outside the organization, the cost factors, and the technological evolution.

- **Robotic Process Automation (RPA) powered continuous controls testing:** Given the increased checks from regulators and the varied new risk sources, controls testing on data samples in no longer recommended. Instead, today organizations need to thoroughly test each of the risk controls using multiple scenarios. This will help avoid anything to slip through the cracks!

  For example, in the vendor management space, this would entail validating that the PO is not created and approved by the same person; and whether the approver has the approving authority in the specific region. As another example, in timesheet approval report verification, there would be need for validating the submitter and approver information.

  Infosys recommends the use of RPA based bots which can be effectively leveraged in the above-mentioned cases – it would help automatically validate each line record within seconds and share the test outcome with evidence, which can be stored and timestamped for future references.
- **Engaging the first line of users:** For GRC to be truly people centric, it needs to be easily accessible to all of the concerned staff. The days of access based systems/processes that are used for triggering issues/observations are past. Instead, all users and employees should be enabled to report an issue/ incident and track it to closure.

  In our view, technology interventions such as chatbots and outlook plugins can be effectively used to ensure that means are created for all employees to report and track any issues/risk they encounter or foresee. These incidents can then be plugged into the central GRC system for central tracking.
- **Predictive analysis to detect risks before actual breach:** Organizations can leverage Artificial Intelligence (AI) capabilities to analyze data and come up with credible leads that can be tracked to proactively avoid the incident/issue before it occurs.

  AI can help transform this space by giving pointers to cases where potential breaches can happen - with the help of embedded analytics within the business logic, including prescriptive analytics, and moving towards building a continuous auditing program. This will indeed transform the "business of auditing" to drive the audit process and risk identification.

Navigating the document minefield with Machine Learning (ML) - An internal audit use case: Illustrative example

Problem statement: Internal Audit and Data Analytics division in financial institions typically handles large amount of data (both structured and un-structured) and documents to define and install internal checks and controls in order to identify signs of fraud. The solutions installed (although automated) lack operational excellence, intelligent output and involve regular manual interference.

Proposed Solution: The historical alerts, document insights, KPIs, threshold levels and data trends from the markets can be analyzed by ML algorithms to use its predictive power to forecast new KPIs/ thresholds and further optimize them for real time fraud detection. This is a natural step in the right direction. KPIs and thresholds will consequently offer predictive and prescriptive indicators, not just rearview-mirror reviews. Data-driven organization that leverage these advances by reconceiving their thresholds will enjoy distinct advantages.

AI/ML Model suggests control levels

- ML models suggests Controls, KPIs and Threshold more dynamically, based on historical behavior
- ML model invokes workflows to get the suggested strategies approved and accordingly deploys
- Based on the actions taken on the suggested strategies of the ML Model, the model improves further

AI/ML Model manages Incident Management Process

- ML models suggests recommended actions, based on historical data. The model improves, with new actions/ overrides
- For those actions which can be automated, ML model invokes required workflows, hence reducing the number of incidents that analyst has to work upon manually.
- Identifies false positives and automatically closes them, hence further reducing the number of incidents that analyst has to work upon manually.

Exhibit 2 – AI/ML enabled solution

Conclusion

Innovation and automation are the cornerstones of any GRC Digital transformation. Having said that there is no one-size-fits-all GRC solution for organizations – as all such transformative interventions come at a cost. It is therefore important for firms to conduct thorough cost benefit analysis before they embark on their GRC transformation journey!

About the Authors

Amit Khullar

Segment Lead , Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Amit leads Risk & Compliance practice for Infosys Financial Services unit , and is engaged in solution consulting and delivery management for transformational initiatives across various Infosys clients.

He has more than 20 years of experience across the financial services industry and IT consulting. Over the years, he has managed many complex business transformation programs and initiatives for global financial institutions across the banking, capital markets, risk management and regulatory compliance segments. He can be contacted at Amit_Khullar@infosys.com

Navdeep Gill

Principal consultant- Lead GRC COE , Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Navdeep is currently leading the GRC COE for Financial services Domain Consulting Group and is engaged in solution consulting and delivery management for transformational initiatives across various Infosys clients

She has more than 12 years of experience across the financial services industry and IT consulting. She has been a part of multiple transformational programs in the Risk and compliance space- with customers globally . She can be reached at Navdeep_gill@infosys.com.

References:

- https://www.oceg.org/about/what-is-grc/

For more information, contact askus@infosys.com

Infosys®
Navigate your next