
BEING RESILIENT
MOVING TOWARDS A NEW ERA OF CORPORATE COMPLIANCE
Infosys®
Navigate your next
MetricStream
PERFORM WITH INTEGRITY™
BEING RESILIENT. THAT'S LIVE ENTERPRISE.

Corporate Compliance

The corporate compliance function is associated with ensuring compliance to policies and the coordination of the organization's business functions built on a robust integrated policy-based standard operating procedure and audit management functions which depend on people, process and technology.

A strong corporate compliance framework and principles that govern risk controls are essential to report observations and manage/recommend actions related to potential non-compliance, negligence, or impropriety during uncertain times.

The severity of the current Covid-19 crisis has been very profound and the global economy has already started showing signs of slowing; the loss recovery for most corporates has already eclipsed the global recessions from 2008 and the dot com bubble burst at the beginning of the millennium. Unlike the 2007 financial crisis which was centered on financial sector in its origin and resolution, the current COVID-19 situation is operationally centered. Which further means that the impact of this crisis is mainly driven by the disruptions in business operations due lockdowns, government restrictions and health warnings. Thus, the financial packages provided by governments worldwide are not really contributing to a direct recovery but simply mitigating the effects of the disruptions. Once the actual recovery begins, GRC/IRM would provide view of intertangled risks (i.e. operational, regulatory, policy, business continuity, third party and compliance) that enterprises must overcome to overcome this crisis.

A Chief Compliance Officer is responsible for supporting compliance policy management which includes sourcing/ analysis of raw data and information from various regulators, legal experts, industry bodies and corporate best practices to sustain organizations' operational efficiency, business continuity, loss recovery and overall responsiveness to rebound from the impact of the COVID – 19 outbreak.

The role of Corporate Compliance Officers is becoming increasingly important to manage the crisis and its consequences through a data driven approach in identifying specific causes and executing historical review simulation to prevent risks from accelerating into high impact levels. Below are some of the critical compliance management preparedness aspects in terms of people, process and technology.

Compliance Preparedness: Pillars of Corporate Resilience

People

At the time of this crisis, when large corporations are reeling, it is important to abide by ethical and practical policies to safeguard and enforce ethical employee behavior within the organization, relationship with government officials, shareholders, and business partners to maintain integrity of corporate values. There are key questions around the creation of a virtual workforce, ensuring that there are plans for seamless workforce return, and seamless operations.

Process

The various compliance process objectives should align with the overall corporate GRC vision to have focused impact on enabling/ improving/updating existing business resilience plans- including business continuity management, third party risk management, physical asset security, seamless operations across key business processes, data security etc. in line with communication from regulatory bodies and local governments.

Technology

Data assessment, electronic forms of evidence, news feeds, crisis management systems, virtual collaboration tools, modernization of technology infrastructure, supply chain management and implementation of risk controls are essential to detect any inconsistencies in compliance systems which may impact reputation, brand and recovery in operations, to ensure continued regulatory compliance and reporting at times of the COVID – 19 outbreak.

Moving Towards Corporate Resilience: Vertical Risk Visibility- IRM

In order to be more resilient enterprises will have to revisit their entire GRC framework as they go through this forced transformation to address the new evolving business model. What's also important for business to restart and regain the lost ground is the need to look at risks both vertically and horizontally.

They will need a common risk view across operations, strategy and technology- hence the forced shift towards Integrated Risk Management (IRM)- aided by principals such as a risk-informed strategy, digital risk management and rapidly changing global ecosystems

a. Information Technology Risk & Compliance Management

The survival of an organization during this challenging time is very much lockstep in managing information technology risk and compliance management and how effectively it shares, updates, prioritize policies, actions to deliver interim IT

External Document © 2020 Infosys Limited

operations, infrastructure availability and support pending full resumption of business and to recover from the impacts of an adverse scenarios. The operational resiliency expected would be to –

- Identify risks through IT related measurement strategy (Metrics, Indicators, Computation Methods). Leverage internet news feeds from regulatory bodies, third-party providers, government & quasi government health agencies to forecast interim IT operations plan for information systems recovery plan and decisively implement emergency operating procedures to allow workforce to resume working remotely
- Implement a data storage, security and retention plan to manage information throughout the information life-cycle. Implement classification schema for access, use and transfer of data. Revise storage, retention, disposition and retrieval of information guidelines
- Leverage the digital technologies like AI/ML to ensure key process controls are automated. The monitoring of external regulations, delegation of authority of policy and documentation changes and regulatory requirement changes across geographies could be automated through Robotic Process Automation (RPA) for policy authoring, communication and storage
- Adding predictability to the IT processes using Machine Learning models- to be aware as much as possible of possible distress scenarios in future i.e. when the next ATM failure will occur
- External reporting to regulators and other stakeholders can be revised to define updates to dashboards, alerts and the appropriate level of details/ abstraction for scope of responsibility to increase ability to respond effectively based on a broad network of information sources. Thus, removing any risk of non-compliance even in testing times
- Building robust collaboration platforms to cater to the needs of a virtual workforce
- Secure cloud-enabled infrastructure and security practices to ensure minimal infra impact in future

b. Managing Third-Party Risk and Business Continuity Planning Management

- Measurable indicators and thresholds are essential to be revisited in third-party risk management to protect organization from non-compliance or misconduct by vendors
- Leverage financial methods including insurance, establishment of reserves including supply chain that, may be contingent upon obtaining insurance from third-party vendors that they would remain solvent at the time of this pandemic. Supplier contracts have to be revisited to ensure compliance to operate within the regulated industry requirement during the pandemic
- Identify risk trends faced by vendors based on industry, workforce size, and geography and monitor changes in underlying factors to predict any potential disruption to business continuity
- Short-term vs long-term planning to analyze vulnerability considering the likelihood and impact to third-party vendors' business operations so that the organization is not exposed to threats impacting immediate business continuity
- Stress testing the current plans to ensure the breaking point is well understood across the enterprise and putting an action plan in place to mitigate the same

c. Policy & Documentation Compliance Management

- External regulations monitoring: Identify international, national and financial industry regulations to collect and interpret regulatory change data to incorporate in relevant corporate policy guidelines for employees, third-party, government, stock-exchange notifications, IT governance et al. These guidelines should be adhered to and abided by the workforce in stakeholder relationships, working with regulators, contract employees, localization of policies across geographies et al
- Assess impacts on business continuity by implementing corrective controls based on measurable data including guidelines to operate in challenging times
- Be consistent in policies and documentation and the dissemination of the same should be purposeful to align with the overall organizational objectives to comply with applicable laws, minimize conflicts of interest, maintain transparency and provide accountability by senior management
- Awareness of policy changes should be swiftly enabled through conference calls, policy training modules, helplines and the availability of compliance officers to respond to inquiries from internal and external stakeholder commitments
- Establish mandates and standards for doing business in uncertain times to improve trust, confidence, and reputation

d. Audit Compliance Management

- Define independence from senior management for independent assurance to the board and shareholders to audit and monitor compliance objectives. Re-define senior management roles and accountability to ensure Compliance Officers are able to champion the management of business continuity policy guidelines
- Ensure continuity in accountability of audit function through well documented compliance guidelines segregating roles of the audit team in ensuring the highest levels of corporate governance standards
- Define a clear communication strategy – for both external and internal communications
- Report defective controls and any alleged misconducts while operating in a time of crisis to ensure transparency in operations
- Evaluate periodically thresholds, organization change management, at a pace to keep up with new regulatory changes and without disrupting the operating model of respective business functions is essential
- Work towards providing exceptions and waivers without compromising any local, national, international regulations or laws to operate with rigor during the implementation of business continuity intended to identify any non-compliance

External Document © 2020 Infosys Limited

Way Forward

Although there have been pandemic threats in the past, COVID-19 is the first one to fully crystalize in many countries at the same time. As a result, there will be lessons for boards, senior managers, and all three lines of defense to learn from the current situation. The stressed financial markets and tightening liquidity has begun taking its toll on corporate balance sheets. The role of the GRC/ IRM function has never been in so much spotlight, as the compliance management and operation resiliency of organizations are put to test to their limits. Thresholds in risk controls are being re-examined and compliance policy management is at the forefront of every executive's mind. The continuous and rigorous preparedness in ensuring regulatory compliance obligations are essential to the very survival of organizations at these very challenging times to provide a realistic path to recovery while the world grapples with the new normal.

Offerings like GRC provided by Infosys and MetricStream, will play a key role here, by helping enterprises navigate their next in Risk and Compliance.

About the Authors

Sarojit Mazumdar

Sarojit has 25+ years of business development, consulting and program management experience in the Banking and Financial sector. He has built a strong network of trusted partners and is currently managing the Strategic Partnership and Alliances program at MetricStream. He can be reached on smazumdar@metricstream.com

Binil Roy, Principal consultant- Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys Ltd

Binil is a GRC SME and practitioner with overall 19+ years' work experience. He is focused on Enterprise Risk management and is very closely tracking new developments in GRC domain. His primary objective is to provide meaningful advice in the fields of GRC Blueprinting, GRC Vision and Road-map definition, Product Implementations to follow a process driven approach to meet business goals of enterprises. He can be reached at Binil_Roy@infosys.com

Navdeep Gill, Principal consultant , Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Navdeep is 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 13 years of experience across the financial services industry and IT consulting. She has lead multiple transformational programs in the Risk and compliance space- with customers globally . She can be reached at Navdeep_gill@infosys.com.

References

GRC Capability Model Red Book

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2020 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.