ISOLTX-GRC-A™

Future Proof your Governance, Risk, Compliance and Assurance (GRC-A)

Article Written by: Nico Snyman

Founder and Chief Executive Officer (CEO)

Crest Advisory Africa (Pty) Ltd

MBA, Fellow-IRMSA, M.I.S

PECB: Lead Auditors Accreditation:

ISO 22301, 31000, 27001, 18788, 19600, 9001, 14001, 45001, 37001, 55001, 22000, 28000, 13485, 30301

Advanced Auditing Techniques (AAT) and Internationally Certified Train the Trainer

Table of Contents

Introduction

The GRC environment has been growing exponentially over the past 10-15 years. The higher demand for Corporate Governance and reporting to Executive and Boards has created a need in the market to constantly grow the GRC software environment. Systemisation and Automatisation of the Risk, Compliance, Business Continuity, Audit and other governance environments with the latest requirement, Combined Assurance, has evolved into an extremely demanding and ever-changing landscape for Corporate Governance, whether in the public sector or in the private sector.

This requirement is a constant challenge for software developers, as they need to understand the need of governance, interpret the requirements and if there is a need expressed in the market, that they can respond to it. This requires constant Research and Development (R&D), and as we all know, R&D is extremely expensive. For this reason, the GRC landscape is riddled with software, but do they address your specific need, and can they be easily configured to provide the outcomes needed for this evolving environment?

What is GRC and GRC-A?

GRC is defined [1]*as "an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness".*

This is on GRC, but what about GRC-A? What is the A? A is for Assurance and assurance is defined [2]as follows:

The diligent application of mind to evidence, resulting in a statement or declaration concerning an identified subject matter or subject matter information, and that is made for the purpose of enhancing confidence in that subject matter or subject matter information.

Assurance includes, but is not limited to, assurance engagements performed by independent, external assurance service providers (such as the external auditor) in accordance with the International Auditing and Assurance Standards Board's International Engagement Standards. Such assurance "means an engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria".

Assurance furthermore includes, but is not limited to, assurance provided in terms of the International Standards for the Professional Practice of Internal Auditing, namely, "an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organization".

What are the Tools for GRC?

The primary purpose and objective of any GRC software is to automate much of the work associated with the documentation and reporting of the risk management and

[1] Nicolas Racz, Edgar Weippl and Andreas Seufert in their recent research paper 'Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)

[2] King IV Report on Corporate Governance™: 2016

compliance activities that are most closely associated with corporate governance and business objectives.

The primary end users include internal auditors and the audit committees, risk and compliance managers, and accountable executives. The key functions of GRC software are usually the following:

- **Policy management** features that include a specialised form of document management that enables the policy life cycle from creation to review, change and archiving of policies; mapping of policies to mandates and business objectives in one direction, and risks and controls in another, as well as the distribution to and attestation by employees and business partners
- **Risk management** functions that support risk management professionals with the documentation workflow assessment and analysis reporting visualisation and remediation of risks (as defined in ISO31000). This component focuses generally on risks and incidents follow-up but may also collect data from risk analytics tools (Credit Risk, Market Risk, etc.) to provide a consolidated view of risks
- **Compliance management** functions that support compliance professionals with the documentation, workflow, reporting and visualisation of control objectives, controls and associated risks, surveys and self-assessments, testing and remediation. At a minimum, compliance management will not only include financial reporting compliance (e.g. SOX compliance, King IV™).
- **Industry specific management** functions, this include the various adopted ISO standards, as the best practices in the international community. (e.g. ISO 9001, ISO 22301, ISO 18788, ISO 45001, etc.)
- **Audit management** functions that support internal auditors in managing work papers, and scheduling audit-related tasks, time management and reporting

Silo Approach to GRC

The current software landscape offer ERM, Audit, Compliance, Incident Management systems which does not speak to each other, as the methodology for each are

different. This is called a **Silo Approach to GRC**[3], where the total Universe could not be measured at once, to provide Assurance on various levels of the organisation.

The standard approach in the market is to work from Strategic Risk Registers, to Divisional Risk Registers and Operational Risk Registers, if this functionality is available and the licence costs are not to exorbitant.

This means that it is either a Top Down measurement approach with a selective view of the Risk-, Compliance-, Audit-, BCM Universe. Based on this selective data, decisions are made in terms of strategy, corporate spend, etc.

And if the methodology model is not up to standard, the GRC system, in the silo it is reporting on, will be having a lack of trust.

What is the Corporate Governance Need?

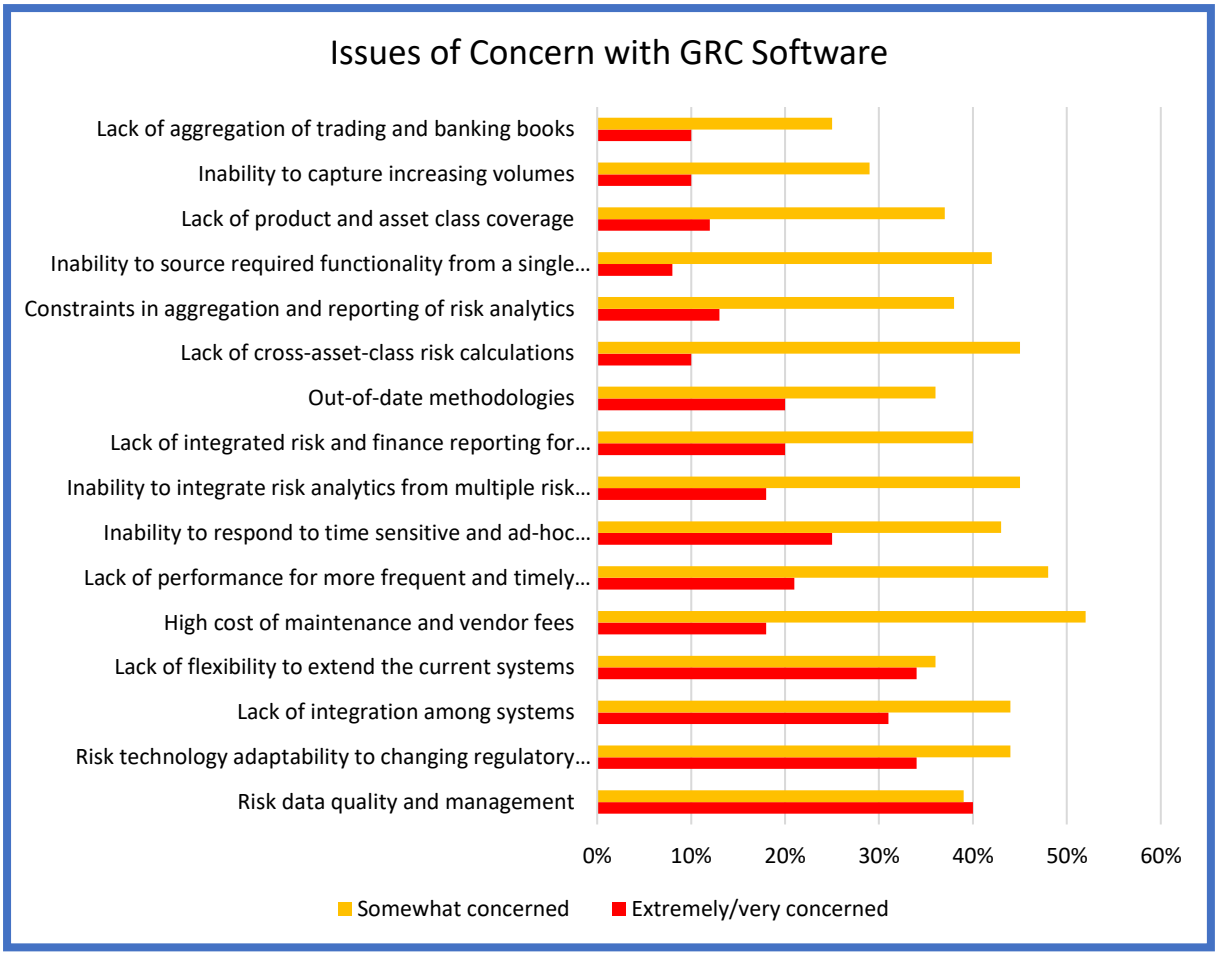
During many sessions with Boards, Executive committees and Management structures, we have realised that there is a tremendous need for: What do we need from a System?

The need for a GRC technological solution is there, but the question remains: which technological tools will be able to provide the appropriate solution?

The current systems, as described as Silo'd, face challenges in terms of fulfilling the need and secondary, can they be integrated with other systems? The answer to this is No!

The graph below indicate the concerns from the industry

[3] NM Snyman: MBA, ICMSA: 2020



The data collected tells a telling a story of Uncertainty. From the risk Data collected and Management, with an Extremely Concerned rating of 40%. This is the norm in the industry.

Corporate Governance Industry driven to technical functionality, not subject matter experts

Most of the systems we encountered in the market is IT companies, with technical expertise of the systems functionality, but little knowledge of the various disciplines. This is a huge gap, as the out of date methodologies are configured and not challenged, implemented and rolled out and this creates a false sense of Assurance.

Software in this sector is build as a framework, hoping and believing that the entity the software is sold to knows what they need to know and are mature enough to upgrade to systematisation. This is often not the case, and the Model risk continuous.

ISOLTX-GRC-A™: Integrated Management Systems (IMS)

ISOLTX-GRC-A™ is unique in this space, as it takes the methodologies of various disciplined, ISO, SOX, King IV, Audit (IPPF and ISO 19011) and integrates it into one comprehensive system.

This is providing a standardised approach to what is needed from each system and measuring the health of each of these systems separately and collectively.

The system makes provision for Application Programming Interface (API), to integrate the various governance software into one system and to provide the best available analytics and reporting on this software.

Artificial Intelligence (AI), Machine Learning (ML), etc

AI and ML is the future of any software and if your current GRC software do not provide you with a roadmap in this regard, it will be outdated in the next 2-5 years and you as an entity, driving Corporate Governance and Combined Assurance, with have a quantum leap to overcome, as your reporting will be limited and would lack, **suitability, relevancy, adequacy, effectiveness and efficiency.**

The Way forward:

ISOLTX-GRC-A™ drives **Performance and Certainty**. ISOLTX is GRC-A software developed by two industry leading partners, specialising in internationally recognised and accredited Training, Advisory Services and Management System Certification (MSC) entity specialising in Management Systems, whether ISO (Internationally), to King IV or Sorbian Oxley (SOX). The second party is a leading University with all the R&D and technical skills needed to build and configure your specific needs.

ISOLTX-GRC-A™ is part of the CAA offerings as a Platinum Accredited Partner of the Professional Evaluation and Certification Board (PECB), based in Canada, under licence of the International Accreditation Service (IAS) (California). This Elite status and accreditation represent the professionality CAA addresses every assignment.

We provide all the various end to end services to drive business, which includes a variety of Management System Toolkits, specifically designed for each standard.

Contact ISOLTX:

ISOLTX-GRC-A™ can be contact on:

Email	info@isoltx.com
Website	www.isoltx.com
Telephone: Office	010 447 3540