May 2023

Lucara Botswana

Best in Class Enterprise GRC Management
Small Enterprise

CASE***STUDY***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organisations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Lucara Botswana

Best in Class Enterprise GRC Management
Small Enterprise

The Need for Integrated Governance, Risk Management & Compliance

The physicist Fritjof Capra stated:

"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."

Capra was making the point that ecosystems are complex and interdependent. They require a holistic, contextual awareness of the intricacy of their interconnectedness as an integrated whole, rather than a dissociated collection of systems and parts. Change in one area has cascading effects that impact other areas and the entire ecosystem. The business operates in a world of chaos. In chaos theory, the "butterfly effect" means that something as simple as the flutter of a butterfly's wings in the Netherlands can create tiny changes in the atmosphere that have a cascading effect that can impact the development and path of a hurricane in the Gulf of Mexico. A small event develops into what ends up being a significant issue.

Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalization, distributed operations, competitive velocity, technology, and business data encumber organizations of all sizes. Keeping business strategy in sync with the accelerated pace of change is is a significant challenge for boards and executives, as well as management professionals throughout all levels of the business.

The interconnectedness of objectives, risks, resiliency, and integrity require 360° contextual awareness of integrated governance, risk management, and compliance (GRC). Organizations need to see the intricate relationships of objectives, risks, obligations, and controls across the enterprise. It requires holistic visibility and intelligence of risk in the context of objectives. The complexity of business – combined with the intricacy and interconnectedness of risk and objectives – necessitates that the organization implement an integrated GRC management strategy.

According to the OCEG definition, GRC[1] is, "a capability to reliably achieve objectives [governance], while addressing uncertainty [risk management], and act with integrity [compliance]." There is a natural flow to the GRC acronym:

1 *GRC official definition in the GRC Capability Model, published by OCEG*

- **Governance – reliably achieves objectives.** The purpose of governance in GRC is to set, direct, and govern the reliable achievement of objectives. Objectives can be overall macro-level but also can be divisional, department, project, process, or even asset-level objectives. Governance involves directing and steering the organization to achieve those objectives reliably.

- **Risk management – address uncertainty.** ISO 31000 defines risk as "the effect of uncertainty on objectives." Good risk management is done in the context of achieving objectives; to optimize risk-taking to ensure that the organization creates value. This is the function of GRC that addresses and mitigates against inevitable uncertainty and threats while operating in a sustainable and calculated manner.

- **Compliance – act with integrity.** The compliance function of GRC is more than regulatory compliance, but the adherence and integrity of the organization to meet its commitments and obligations. These commitments and obligations can be from regulations but also can be found in ethical statements, values, code of conduct, ESG, and contracts.

The Focus is on an Integrated GRC Architecture

The world of business is distributed, dynamic, and disrupted. It is distributed and interconnected across a web of business relationships with stakeholders, clients, and third parties. It is dynamic as the business changes day-by-day and must respond and adapt to evolving environments. Processes change, employees change, relationships change, regulations and risks change, and objectives change. The organization requires a holistic, contextual awareness of GRC – rather than a dissociated collection of processes and departments. Change in one area has cascading effects that impact the entire ecosystem.

This interconnectedness of business drives demand for 360° contextual awareness in the organization's GRC processes to reliably achieve objectives, address uncertainty, and act with integrity. Organizations must see the intricate intersection of objectives, risks, and boundaries across the business. Gone are the years of simplicity in operations. Exponential growth and change in risks, regulations, globalization, distributed operations, competitive velocity, technology, and business data impede the ability of the business to be agile in times of uncertainty.

This challenge is even more significant when GRC management is buried in the depths of departmental processes and addressed inconsistently from different organizational silos and not as an integrated discipline of decision-making that has a symbiotic relationship on the performance and strategy of the organization.

Organizations are focused on developing GRC related strategies and processes supported by an information and technology architecture that can deliver complete 360° insight into risk and compliance. The focus is to deliver:

- **Interconnected risk.** Organizations face an interconnected risk environment and risk cannot be managed in isolation. What started in one area of risk exposure

cascades to others. The recent pandemic has shown, as a health and safety risk had downstream risk impacts on information security, bribery and corruption, fraud, business and operational resiliency, human rights, and other risk areas.

- **Objectives are dynamic.** Adapting to risk events means that businesses need to modify their strategies, departments, processes, and project objectives to address new concerns and possible threats. Objectives become dynamic in reaction to changes in risk exposure. These had to be monitored amid uncertainty in a state of volatility and change.

- **Disruption.** Business is easily disrupted, from international to local events all along the supply chain and extended enterprise. Organizations need to be resilient during disruption with the ability to be agile and resilient in business strategy and operations.

- **Dependency on others.** No organization is an island. The disruption and the interconnectedness of risk impact more than traditional employees and brick-and-mortar businesses but also the range of third-party relationships the organization depends upon, as well as clients. Organizations must address GRC, particularly risk, resiliency, and integrity across the extended enterprise.

- **Dynamic and agile business.** Organizations need to react quickly to stay in business. This requires agility in changing strategy, processes, protecting human resources, employees, and technology. Change also introduces new risks that must be carefully monitored and managed. Organizations need to create an agile foundation that can be flexible in order to meet ever evolving challenges and to bend without breaking.

- **Values defined and tested.** In a dynamic world, organizations strive to align their corporate behavior to ensure their core values demonstrate good corporate citizenship within their communities. From treating employees and customers fairly to how they address human rights such as inclusivity and diversity in their business, operations, and diligence in third-party relationships.

The Bottom Line: In the end, organizations need to reliably achieve objectives, manage uncertainty, and act with integrity and this requires a 360° view of governance, risk management, and compliance within the organization and across its relationships that is supported by an integrated information and technology architecture.

Lucara Botswana

Best in Class Enterprise GRC Management – Small Enterprise

Lucara Diamond Corp. is a Canadian diamond mining company headquartered in Vancouver, a 100% holding company of Lucara Botswana. Lucara Botswana operates the Karowe mine situated in Letlhakane village, Botswana, operating mining production and exploration under a mining license issued in Botswana. The Lucara Botswana Karowe

mine is one of the world's foremost producers of large, high quality, type IIA diamonds in excess of 10.8 carats.

Prior to 2019, Lucara Botswana (Pty) Ltd ('hereafter referred to as Lucara) had a siloed view of risks that were viewed at a department-specific level and not at a strategic level. Furthermore, there was no formal Enterprise Risk Management framework and methodology in place.

So, although risks were captured into an Excel spreadsheet, there was no collective ongoing view of the risk profile and analysis, trending and forward-looking insights into the current and emerging risk profile and tracking of actions was not visible to all.

Additionally, implementation and application of concepts like risk tolerance, appetite and risk mitigation was not organizationally understood and consistently applied.

The Governance and Assurance (G&A) department was established in 2019 to ensure risk eloquence for an intelligence driven organization. The risk management approach which was in practice before the establishment of G&A was fragmented across all business units and as such there was no standardized methodology for Risk Management. The establishment of the G&A department came with the adoption of an Enterprise Risk Management Framework and Policy as well as the introduction of a Governance, Risk and Compliance software solution, supplied by CURA Software.

The CURA system enabled a centralization and standardization of Risk Registers. Therefore, through the CURA system Lucara's G&A has managed to demonstrate to the Board and Audit Committee that the organization is in compliance with the right corporate governance framework and established appropriate compliance practices.

To address this challenge, Lucara focused on Enterprise GRC Management strategy, process, and technology . . .

Enterprise GRC Management Strategy

The critical aspect to address strategy was to align the organization from a foundational perspective. An Enterprise Risk Management Project was initiated that resulted in the formulation of an Enterprise Risk Management Framework and Policy.

This process took approximately four (4) months with various engagements from a Board perspective and with key stakeholders like the Managing Director, General Manager and Chief Financial Officer to gauge views on risks. Lucara used an external professional service provider to assist in the execution of this project.

The nature of business Lucara is engaged is Diamond Extraction and Sales. Governance and Assurance management came up with a Risk Management and Diamond Control internalizing program which was executed in phases.

Phase 1 involving establishing a baseline to understand the view of people towards Diamond Control and Risk Management in the workplace by conducting a survey at the

targeted levels of employees within the scope of the program. The survey was sent out in order for Lucara to understand the broader organizational views about:

- Risk Management to Self and Business
- Responsibilities for Self and Team,
- Lucara's Approach to Protecting Self and Business,
- Improved Integration for Diamond Control and Risk Management.

Phase 2 involved conducting a workshop consisting of operational management and employees during which the survey results were analyzed and interpreted by the group. During this review the opportunities and challenges derived from the survey were discussed and an action plan developed to address the challenges and opportunities for improvement.

Phase 3 was to ensure effective execution and measurement of an internalization approach. A workplace risk representative forum that meets on monthly basis was established and chaired by departmental Risk Champions. The Risk Champions report to the local operational management team. The Departmental Risk Champions have a committee which meets on a quarterly basis and provides reports to the Chief Risk Officer through a forum chaired by the Chief Risk Officer. The forum is made up of representatives of all departments at both Karowe and Corporate Office operations.

The ERM framework represented Lucara'scoordinated plan for risk management across the entire company to effectively deal with the uncertainty of associated risk and opportunity, thereby enhancing its capacity to build value.

The following factors required consideration when integrating ERM into Lucara's decision-making structures:

- Aligning risk management with business objectives at all levels of Lucara
- Introducing risk management components into existing strategic planning and operational practices
- Including risk management as part of employees' performance appraisals
- Continuously improving control and accountability systems and processes to take into account risk management and its results.

The framework specifically addresses the structures, processes and standards implemented to manage risks on an enterprise-wide basis, in a consistent manner. The standards further address the specific responsibilities and accountabilities for the ERM process and the reporting of risks and incidences at various levels within Lucara.

The Lucara ERM Framework has been developed to ensure strong alignment to the following globally recognized leading frameworks for ERM:

- Committee of Sponsoring Organizations of the Treadway Commission's (COSO)
- Integrated ERM Framework, 2004 (COSO ERM) revised 2018
- International Standards Organization (ISO) - ISO31000, 2009 revised 2018
- King IV Principle 4: "The governing body should appreciate that the organization's core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process"
- King IV Principle 11:" The governing body should govern risk in a way that supports the organization in setting and achieving its strategic objectives".

The strongest aspects of COSO ERM (2018) and ISO31000 (2018) are encapsulated within this document ensuring sufficient guidance is provided on the recommended methodologies that best achieve the objectives of the Risk Management Policy adopted by Lucara.

These methodologies were defined through continued research and development as well as being benchmarked against international best practice. The methodologies transfer knowledge and risk management technologies to and within Lucara, applying a consistent approach, and encourage interaction between the various Lucara departments/ functional areas.

Once the Board was involved and a view of risks at a strategic and governance level were understood, the foundation was laid to create the ERM Framework and Policy that was to be implemented and embedded within the organization.

Enterprise GRC Management Process

To address the processes challenges, the following was done:

- Arrange departmental risk workshops taking the teams through the ERM Framework (Methodology and Policy)
- Provide guidance on how to identify risks and accurately capture them
- Provide insight on looking at current controls (and keeping them at a minimum of a satisfactory level) and then focus on actions that will serve to improve the control levels and bridge any existing gaps to improve control effectiveness.
- Identify and train Risk Champions per department to take ownership of the risk registers and use it to manage their risks more effectively and proactively – both backward and forward looking

- Establish ongoing opportunities to speak about risk in daily/weekly/monthly interaction and not just the quarterly risk board submission

- Provide ongoing support from either the Chief Risk Officer with Heads of Department and/or Risk Champions

Enterprise GRC Management Technology

From the onset of the ERM project, the organization recognized that an automated GRC tool was needed to enable the organization to standardize how risks are identified, assessed, actioned, and reported on.

Furthermore, Lucara needed to identify those GRC service providers that were aligned to our current risk management maturity in that the organization was starting out with the automation of risk management, so were conscious of the cost/benefit that needed to be realized in the initial phases of the transition.

Lucara conducted research into the GRC vendors that ranged from SAP, Barnowl, ACL and CURA and narrowed it down to ACL and CURA. Various demonstrations were held with the service providers to understand their offering and modules and ability to scale-up as the organization and functions matured.

It is equally important for Lucara to have a connection with chosen service providers in their ways of work, approach and methodologies used. The engagement with CURA allowed for a deeper connectedness not just in their GRC offering, but how Lucara and CURA would work together to build the GRC foundation from which Lucara could springboard.

Post engagement with CURA, a project plan and execution strategy were set up and this has continued since the end of 2019. Interactions and engagement with CURA, at a strategic, customer account and helpdesk level, occur at defined intervals or as matters arise, and this has been in place for some time, allowing for direct dialogue with the needed expertise at the time it is required.

The required reliability and agility of the GRC tool and its technology was reached with CURA. The post-implementation service and consulting/advisory became equally important as Lucara scaled up and implemented its modules.

Additionally, the awards that CURA has attained over the years for their products and services and impact on the industry does also provide Lucara with comfort that our service provider is leading in aspects of technology, innovation, and systems.

Benefits Delivered

Lucara was looking to find a GRC fit that would pull in four things, namely:

1. **People** - Enable our people to buy-in to the Methodology and Technology

2. **Process** - Show our people that the process to be followed is straightforward and uncomplicated; Also allow for scalability to move users / areas through a new module (like Compliance or Policy)

3. **Data** – Provide ease and simplicity with which users can capture, view, and assess data

4. **Technology** – Ensure maximum uptime of GRC resource and ability to reach out to resources /helpdesk in a timely manner.

The way the components were integrated, starting with the ERM methodology/ framework, and then finding the most aligned GRC tool to us was the core foundation. Post that, the ability to gain buy-in and commitment to use the tool effectively, without having to look ''under the bonnet to see the engine" and focus on what the user needs is secondary.

Having key people in the business like the Chief Risk Officer, Superintendent of Governance & Assurance and the new addition of a Compliance Specialist helped to have these Risk Drivers that took ownership of various CURA modules and allowed for increased focus of areas and the adoption of the CURA modules by those affected and/ or involved.

One of the most significant benefits seen by Lucara is that it allowed management and risk champions to take enhanced ownership of risk management.

Efficiency

The approach Lucara took can almost be likened to a rapid release of risk anti-bodies. The organization didn't run the risk of going ''all in" when the project was started. A Plan-Do-Check-Act approach was enlisted as each module was started. Lucara ''injected" what was needed first and then observed the response/reaction, before moving onto the 2nd or 3rd phase implementing modules.

Focusing on getting one module in, working, testing, and tweaking before starting on the next was an instrumental shift to the risk culture change too.

This module-relay-race-type build helped Lucara to get the buy-in first by the audit team (as they were essentially the super-users/testers) before engaging the users fully on the risk module. It also allowed for full immersion in the tool and enabled better integration of modules and their interconnectedness (as risk and controls can be used across all modules).

Therefore, time was leveraged in a proactive manner and duplication of effort was prevented across the organization by ensuring scaled testing was performed before dissemination of the tool to the broader team.

From a capital/resource's perspective, Lucara was only billed when each module was properly signed off on and tested to ensure costs were only incurred at the time of

module adoption, as opposed to module procurement. This prevented any resource wastage as user adoption was ensured before committing to any additional capital outlay.

Effectiveness

The approach allows for greater process effectiveness as the users are familiar with the risk management software and how changes to it may impact them. As our ERM Methodology has not changed, their process continues unaffected to mature their controls and actions to the desired level through ongoing discussions on their specific tasks needed to be done to improve their controls.

Agility

The approach allows for greater adoption of change management initiatives when the foundation has been properly set. It also allows for any future roll-out of risk modules or enhancements in the risk management space to be more rapidly accepted, implemented and used due to a positive experience in the initial implementation.

Lucara Botswana (Pty) Ltd Achieved Best in Class GRC Management

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], address uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]. Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve more robust processes that utilize accurate and reliable information. This enables a better-performing, less costly, and more flexible business environment.

GRC 20/20 has evaluated and verified the implementation of CURA at Lucara. It confirms that this implementation has achieved a remarkable case study in how to address Enterprise GRC management with clear benefits achieved.

This approach is best in class. In that context, GRC 20/20 recognizes Lucara and CURA with a 2023 Best in Class GRC Award in the Category of Enterprise GRC Management – Small Enterprise (Under 1,000 employees).

GRC 20/20's Final Perspective

With the Underground Expansion due to come fully into production in 2026 – as Lucara is currently an open pit mine – mining will now also take place underground and as such this environment is new and unfamiliar. Lucara's focus is already forward looking to the underground operations and how it will impact all other parts of the operations including new associated risks.

Additionally, Lucara has received requests from their lenders/financiers for the Underground Expansion for additional information on the operations and this extends to provision of risk/control information that CURA can provide to them.

The company is also further embedding the Compliance and Policy Module with the addition of the Compliance Specialist to the team, therefore greater focus on the view of our Compliance Universe and landscape will start to shape how compliance is managed moving toward a more integrated approach. Lucara recently had the adoption of the Data Protection Act (Data Privacy Act) in Botswana, and the organization engaged the Data Protection Act Commissioner on the aspects to consider in legislation implementation. All these interactions help to shape the future of compliance for Lucara to follow a more integrated approach to GRC.

With the recent certification of the company to be ISO45001 compliant, the need to remain compliant to the SHE standard is critical. To this effect, Lucara plans to continue to use CURA to implement a Compliance Management System which mirrors the requirements of ISO 37301.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com