an overview on why, what and how to implement a

Governance Risk & Compliance framework

nemo iTsolutions

Contents

Why
do we need GRC

Executives main concerns

In every organization, the main concern of the leadership is to have a clear and an effective oversight on the long and short term strategy, the enterprise processes, the available technology and the human resources management. There are some questions like “Do we have a clear view of our company’s strengths, weaknesses, opportunities and threats?” or “Are we in compliance?” that the board of directors seeks for efficient and accurate responses in a regular base. Additionally, control mechanisms result and reporting is crucial for chief directors in order to take decisions. In the figure on the right, there are the main components of the leadership concerns together with some indicative questions that the C-level team is facing regularly.

Strategy

- What are our long term objectives?
- What are our strategies to achieve these goals?
- Do we have a clear view of our strengths, weaknesses, opportunities and threats with regular assessments?
- Do we have an efficient and effective organization matrix?
- Are we agile enough to timely adopt any changes?

Processes

- Are we in compliance?
- What are our risks?
- What should be our response to these risks?
- What are the potential impacts?
- Are we effectively mitigating our risks?
- Do we have adequate reserves in the event of an occurrence?

People

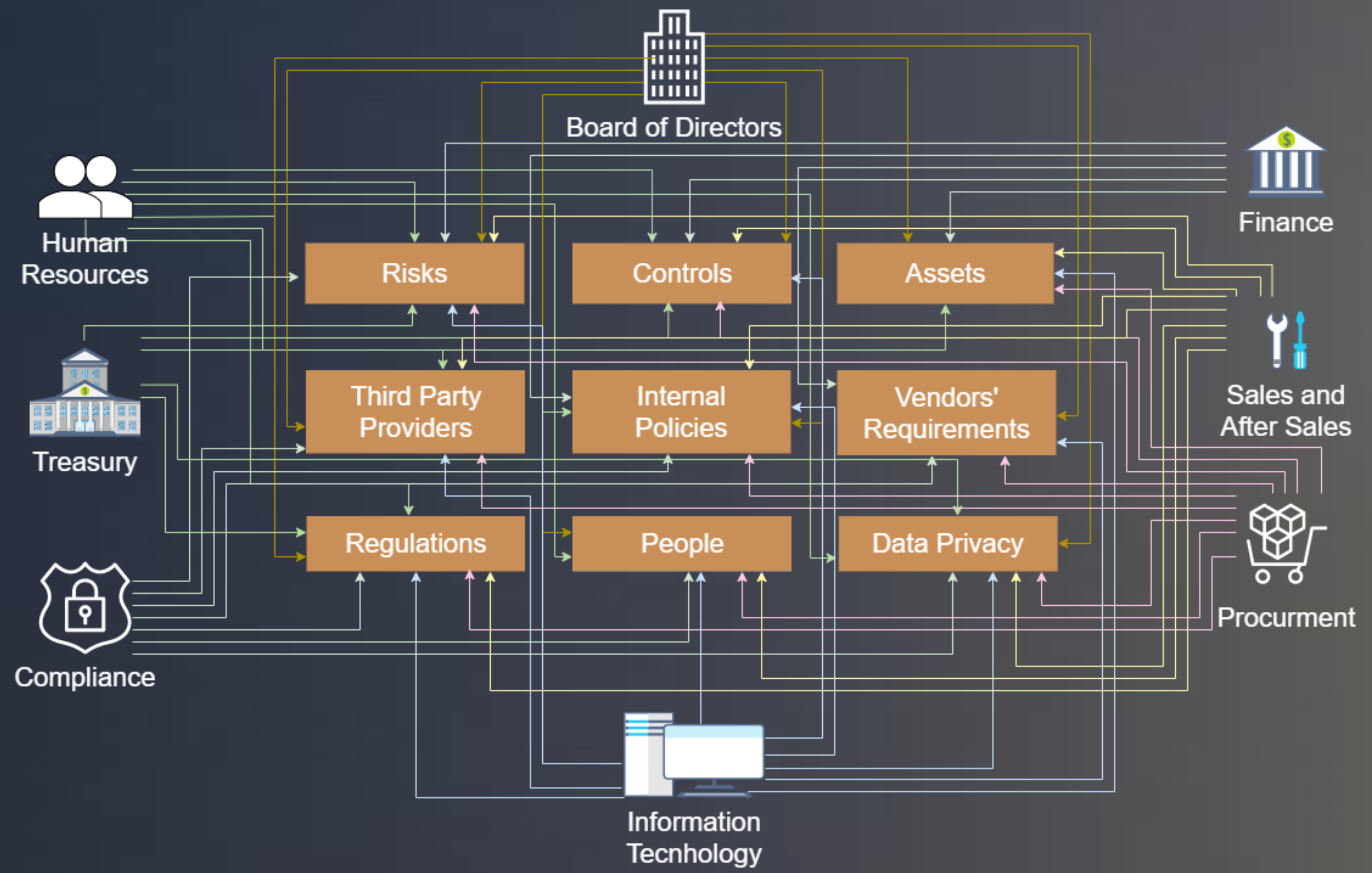
- Are we confident with the level of access of our people across our environments?
- Do our people have clear job descriptions?
- Do we manage digital identities effectively?
- How do we manage the user provisioning and de-provisioning?

Technology

- Are our data safe on premises, on cloud or on heterogeneous environments?
- Are we in compliance with data protection laws?
- Do we follow the standardized best practices?
- Are we in compliance with particular vendors standards?
- Are we facing operational issues?

Why
do we need GRC

Spaghetti Response Approach



Departmental needs

Each department within an organization is facing various risks. These risks can have different flavors like Financial risks, Reputational Risks, Security risks and so on. At the same time all the departments are facing the same risks, but from a different point view.

Besides the risks, departments have to be compliant with regulation requirements and internal policies and to follow the strategic objectives of the top management.

In most of the cases, under this situation each department responds to risks, regulations and strategic decisions by establishing siloed and fragmented policies that lead to ineffective procedures and high cost processes. In the above figure there is a typical structure of this disjointed – **spaghetti** – approach.

Unfortunately, when in an organization each department develops and follows isolated programs, that results to:

- Lack of global visibility of the risks
- Duplication of procedures
- Slow enterprise performance
- High cost for control mechanisms and reporting
- Inability to address third party risks
- Unpleasant high cost drawbacks

What is GRC

GRC is standing for Governance, Risk and Compliance. Some people use to replace Compliance with Control, but analyzing in detail these 3 practices we will realize that control is an essential part of them. The first scholarly research on GRC was published back on 2007 by Scott L. Mitchel where defined as “The integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity”.

A lot of work has been done since then and now, when we refer to GRC, we address a complete framework that aims to help organizations in order to:

- synchronize information and activities across governance and compliance,
- operate more efficiently,
- enable effective information sharing and reporting,
- obtain clear visibility on risks and opportunities
- avoid wasteful overlaps and
- gain effective oversight on strategy, processes, people and technology

It’s obvious though that GRC disciplines are not something new. Organizations have been governed, risk assessed and been in compliance for a long time, so GRC as individual components is not something new. However, the integrated approach of setting up process and practices across organization departments and functions is the key component of the innovation inside GRC.

Many times in discussions related to GRC there is the impression that GRC is a software tool or a platform. Even though there are a lot of vendors providing GRC applications, the installation of a software is not mandatory for the organization to enjoy the benefits of an integrated GRC framework. GRC is a business framework that contains processes, workflows, best practices, risk assessment methods, compliance rules and regulation control mechanisms that help an organization to achieve its objectives with responsibility, transparency, integrity and at minimum cost. If this framework is missing, then installing a GRC tool cannot replace any missing piece of this puzzle. GRC tools are perfect to automating existing good processes.

In the core of any GRC implementation, there is a need for Organizations to define "what they need to know" about their own assets and processes in order to calculate risk and make educated decisions on how to mitigate it.

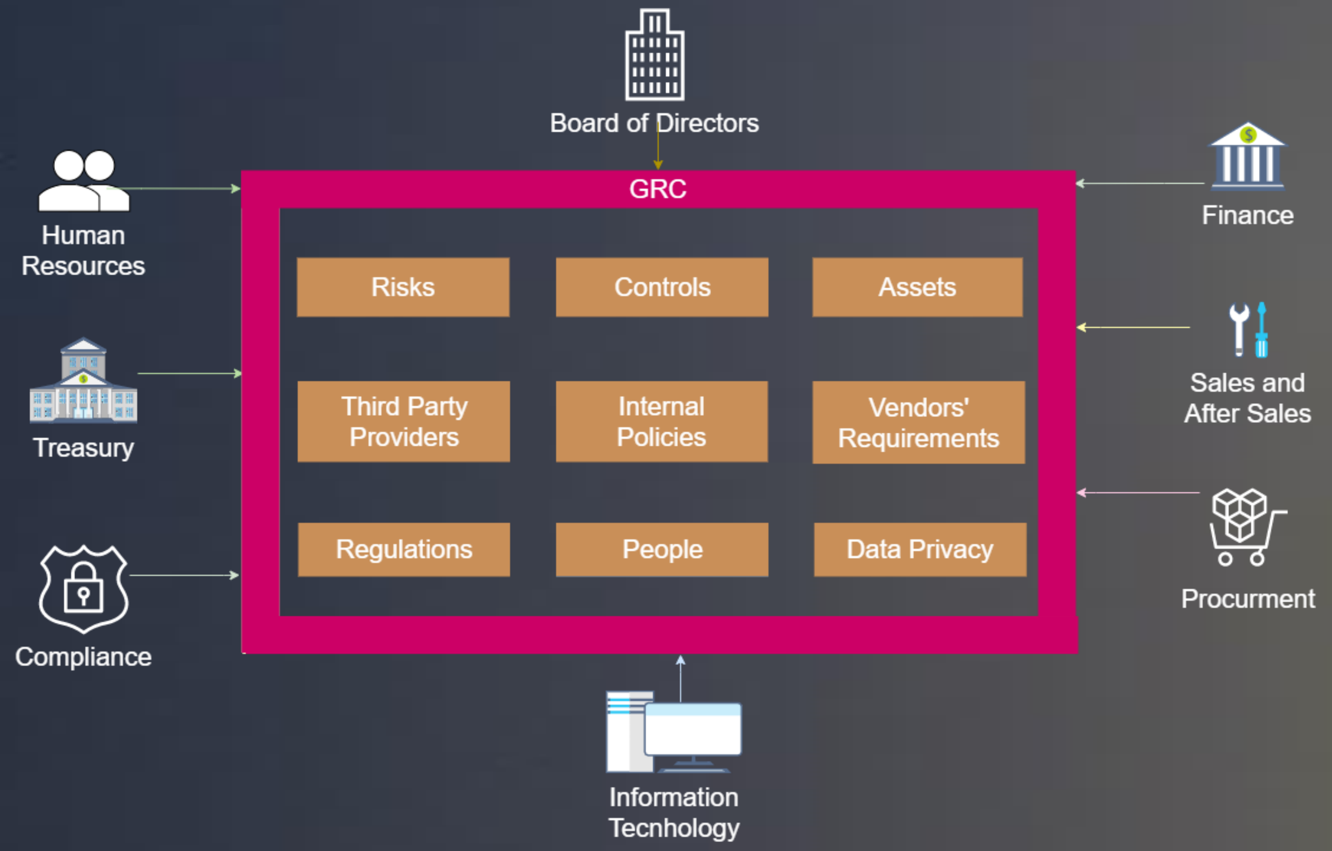
What is GRC

GRC is not an additional department within organization. As we mentioned is a business framework, so the first 2 things we have to define are what is surrounded by this framework and where this framework is addressed to. In other words, we need to clearly define the business functions included in GRC and the business areas that are around and attached to it.

Business Functions Surrounded by GRC framework

Even though each enterprise can follow different approaches in business functions, there are some common components met in every organization:

- **People**, including employees, third party providers (suppliers, vendors, contracted employees), organizational structure, roles and responsibilities
- **Inventory**, including Information Technology and physical assets like hardware, software, networks, physical access keys, etc.
- **Risks**, including all flavors of risks like financial, reputation, operational, security, data privacy, fraud etc.
- **Compliance**, including regulatory requirements (like GDPR, PSD2, SOX etc.), vendors' special requirements (like PCI/DSS), security requirements (physical and non-physical), values and ethics.
- **Policies**, including processes, workflows, controls, strategy, assurance and audit procedures .



Board of Directors

Human Resources

Treasury

Compliance

GRC

Risks

Controls

Assets

Third Party Providers

Internal Policies

Vendors' Requirements

Regulations

People

Data Privacy

Finance

Sales and After Sales

Procurment

Information Tecnhology

Business Areas Attached to the GRC framework

Starting from the top management, we can say that every business area of an organization is attached to the GRC framework like Board of directors, Human Resources, Finance, Information Technology, Procurement, Compliance, Sales and After Sales, Treasury, etc.

What is GRC

Benefits

Cutting Cost

The integrated GRC framework brings real financial benefits as unnecessary spending can be cut.

Avoid duplicated work

Having similar processes duplicated across the business is a hugely inefficient way to operate and GRC can free up whole teams to work on other projects..

Better allocation of resources

Integrated GRC can provide additional information and understanding about the areas that are duplicating work, so it can help to determine more effective direction for the business.

Better capital allocation

Identification of business of redundancy and inefficiency allows financial capital to be allocated more effectively.

Optimization of the Processes

Non – value added activities are eliminated and the value – added activities are streamlined to reduce lag time and undesirable variation.

Business security

Improved operational efficiency by automating common processes and implementing continuous monitoring of controls and exposures to risks.

Faster adoption of changes

Reduce of the response time to regulatory changes and the time to manage compliance activities

Reputation Safeguarding

When risks are managed more effectively, organization reputation is enhanced.

Consistency

Improved alignment of objectives with mission, vision, and value of the organization, resulting in better decision-making agility and confidence.

Transparency

GRC allows the ability to view a more complete picture of the organization and processes, allowing owners to have access and control over necessary content to understand the business unit profile and applicable risks and challenges.

How GRC works

The implementation of a GRC framework is not a standard process. As we use to say is not the case when "one size fits all". Every organization have their own tastes, needs and objectives. However, there are some common rules and practices that are applicable and mandatory during the GRC founding in any organization. The main objective during the introduction of the GRC is to maximize the positive impact and minimize any potential disruption in the implementation period. So first we need to clearly define the people who will get involved in this journey, the roles that these people will have and then to create the detail plan of this transformation including the research, the iteration, the collaboration and the communication.

People

The question is: "who needs to be involved in a successful adaptation of GRC?". The truth is "everybody". Since there are elements of governance, risk management and compliance which go from the very top of a company down to deep within business units and teams, everyone is necessary to be aware. Executives cannot possibly have the knowledge and responsibility for all matters involving risk management and compliance. The management needs to sit together with business unit managers and officers and then to communicate all the changes to their teams.

This chain can be very complex, however we need to keep it as simple as possible, particularly when over-complicated structures already exist within organization.

Of course, this will vary depending on the size and complexity of the business, but what is consistent across all shapes and sizes is the need for effective collaboration and communication and the need for all involved to be aware and mindful of the bigger picture rather than simply their role in it. From the top down, the benefits of GRC need to be communicated as part of a change management strategy to ensure that everyone has bought into the need and expected benefits.

How GRC works

Roles

Board of Directors: Provide oversight, decision-making capacities and clear communication to enable engagement to the chain

Finance officer: He has the overall responsibility for the financial operations and provides the financial drivers for the changes

Risk manager: Identifies and evaluates threats & opportunities and comes up with strategic responses.

Compliance manager: Anyone with responsibility for compliance need to be involved in all planning decisions, driving forward strategies that help the business meet the requirements needed for standards, laws, etc

HR manager: He is responsible for the GRC implementation communication within organization to ensure buy-in. Without the effectively involvement of the HR department any major strategic overhaul is forced to fail.

IT manager: He is responsible for any technological solution is bought in or developed to meet the needs of the GRC strategy. He will also be responsible for the Confidentiality, Integrity and Availability of any information is gathered across the business and how is it delivered where it is needed.

Nemo IT Solutions GRC modules

Governance, Risk management and Compliance have been dramatically reformed the last decade following the entire digital transformation. Traditional and fragmented approaches are fated to fail in front of the innovating challenges like enhanced user experience, big data analysis, cloud computing, artificial intelligence, cyber security. Nemo IT Solutions provide a complete framework consisted by 3 modules

Enterprise module

Classifies all types of risk according to referential internal or external standards like ITIL, COBIT, ISO27k etc. and provides a complete treatment methodology including:

- Risks identification
- Threats repository and Registration workflow
- Risk Assessment process and definition of the Key Risk Indicators (KRIs)
- Organization processes, policies and obligations registration
- Cyber security

Control module

It's a risk-aligned, automated framework that provides real-time high performance control to the organization. Includes:

- Issues and incident management workflow
- Users access control
- Monitoring and auditing plans
- Efficiency alerts
- Standardized management
- Performance dashboards
- Business agility

Reporting module

Reporting module provides an accurate and clear view of the current state of the organization demonstrating to auditors, regulators, and board of directors that all the significant risks and controls are identified, assessed, monitored and reported by a strong governance management.

- Best practices reporting
- Action plans
- Real-time visibility of control effectiveness
- Follow up process

GRC Implementation Plan

1 Current State Assessment

Review the existing framework (every organization practices GRC somehow) and identify the gaps and redefine what governance, risk management and compliance means for your organization.

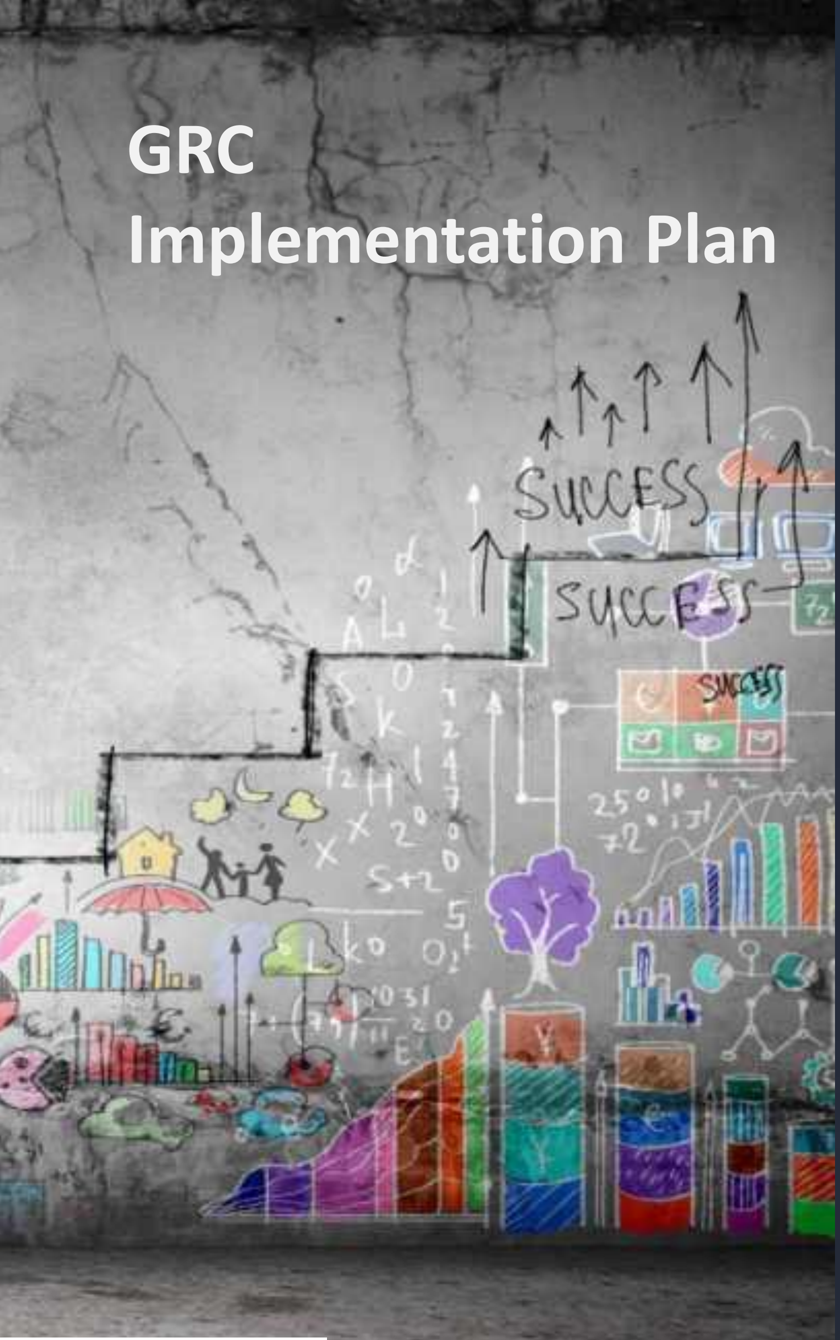
2 Set the Goals

After the current state assessment of the organization we come up with a list of gaps, mitigation actions, proposals and suggestions for improvement. Now we need to analyze these tasks, set the priorities and clearly define the goals of this implementation.

3 Determine Success Criteria

With a refined understanding of the existing landscape, scope and associated business case for the program, carefully crafted success criteria mapped to specific departments and functions will allow project stakeholders to see their own specific expected benefits. Success criteria will take different shapes for various departments. The key is in communicating the criteria to the broader team both before and during subsequent phases of the project.

GRC Implementation Plan



4 Create the Project Plan

Articulate and document a well-defined GRC implementation plan.

5 Implement GRC Practices

Policies, Document management, operational and IT risk management, business workflows, corporate compliance management etc.

6 Continuous Improvement

Implementing a GRC program is not a one-time activity. It is a continuous business practice and must be followed every day across all departments. It is therefore important to closely monitor and ensure that GRC practices are well followed and being matured within the organization. Also, since the business world is highly dynamic, you must modernize your GRC platform and revise your policies regularly to match business, industry and regulatory requirements

Why to work with Nemo IT Solution

In Nemo we are committed to provide an adaptive and future-proof foundation for your enterprise and accelerate your organization’s transformation journey

Our vision is to become a **trusted and strategic partner** to Institutions to entourage them achieve their digital transformation journey.
Our team acts with integrity and honesty, and focus on putting ourselves in the shoes of others. We’re honest, transparent and committed to doing what’s best for our customers and our company. We uphold the highest standards of integrity in all of our actions.

We provide outstanding products and unsurpassed services that, together, deliver premium value to our customers. We achieve our goals without compromising on quality.
We listen to our customer needs, we strive to understand them and deliver beyond their expectations. We treat our customer the way we want our own family be treated.
We build trust through constructive, candid communication that serves the common good. We speak the truth. We believe in each other. Building trust requires confidence, faith, patience and effort. We do what we say we’ll do.

nemo iTsolutions

www.nemo-itsolutions.com

Follow us: in