

POLITECNICO

MILANO 1863

School of Industrial and Information Engineering
Master of Science in Mechanical Engineering



ADDRESSING A SUCCESSFUL IMPLEMENTATION OF A GOVERNANCE, RISK AND COMPLIANCE MANAGEMENT SYSTEM

Candidate:
Luca Zaccari

Matr.: 854112

Supervisor:
Prof. Guido Jacopo Luca Micheli

Academic year 2015/2016

SUMMARY

ABSTRACT (ENGLISH)	4
ABSTRACT (ITALIAN)	5
ACRONYM USED	6
EXECUTIVE SUMMARY (ENGLISH).....	7
EXECUTIVE SUMMARY (ITALIAN).....	16
1. INTRODUCTION	26
1.1 GRC systems and “silo structures”	26
1.2 Tools and guidelines for the selection and implementation of a GRC system	26
1.3 Tips for future development.....	27
2. GRC SYSTEMS	28
2.1 GRC Systems	28
2.1.1 GRC drivers and how the need of an integrated GRC arises.....	28
2.1.2 The benefits of an integrated GRC system	29
2.1.3 Implementation phase.....	30
2.2 Components of an integrated GRC system	31
2.2.1 Governance.....	31
2.2.2 Risk.....	32
2.2.3 Compliance.....	33
2.3 Calculating the ROI of an integrated GRC system	34
2.3.1 Cost estimation	34
2.3.2 Benefits estimation	35
2.3.3 Risk analysis.....	36
2.3.4 Summing up.....	37
2.4 Big Picture for Governance, Risk, and Compliance Platforms.....	38
2.4.1 GRC study	38
2.4.2 Existing GRC evaluation and classification systems.....	38
2.4.3 The new evaluation and classification system.....	39
3. SILO STRUCTURES.....	42
3.1 What is a silo structure and why is used.....	42
3.2 The issues of a silo structure	44
4. PREREQUISITES FOR A SUCCESSFUL IMPLEMENTATION	47
4.1 Top management support	47
4.2 Risk management system	48
4.3 Proactive Risk Management	48
4.3.1 Risk: threat or opportunity?	50
4.4 Enterprise resilience	50
4.5 Nokia-Ericsson Case.....	54
4.5.1 The disruption.....	54
4.5.2 Nokia response.....	55
4.5.3 Ericsson response	55
4.5.4 The results and lessons learned.....	55
4.6 Conclusions.....	56

5. GUIDELINES FOR A SUCCESSFUL IMPLEMENTATION	57
5.1 Motivating and communicating the reasons	57
5.2 Creating a common language	58
5.3 Basic training on risk management	58
5.4 Active staff participation.....	59
5.5 Handle the project in phases	59
6. SUGGESTIONS FOR FUTURE DEVELOPMENT	61
6.1 BYOD Policy	61
6.2 Just Culture	62
6.2.1 <i>Linate accident, October 8, 2001</i>	63
6.2.2 <i>Risk management culture</i>	64
6.2.3 <i>How Just Culture works</i>	64
6.2.4 <i>Creating the necessary conditions</i>	65
6.2.5 <i>What Just Culture can makes for integrated GRC systems</i>	66
7. CONCLUSIONS	67
BIBLIOGRAPHY	68
APPENDIX	70

ABSTRACT (ENGLISH)

This is a literature review project based on the study of integrated GRC systems. It aims to create a document, for the companies interested in integrated GRC systems, by collecting and providing useful information about these platforms (their features, implementation prerequisites, implementation tips, etc.).

This should allow the companies to select and deepen the topics in which are more interested and at the same time to be able to identify all the elements involved in such a project.

In other words this should to be considered as a preparatory work to be uses during the first approach to GRC systems, in order to provide ideas that help the reader to focus on what considers more important or appropriate to his business reality.

The material consulted to create this documents is composed by articles, publication and documents written by consulting companies or experts and interviews to CEOs of companies that have successfully implemented an integrated GRC system and make a continuous and profitable use of it.

The form and structure of this document have been designed to meet the needs of the readers, making an extensive use of lists in order to facilitate the reading and providing business cases or secondary data in order to support the discussion with practical examples.

The overall work is divided into three main parts.

The first one is about GRCs (What are they?, How do they work?, What benefits could they bring?, etc.) and the problems of "silo structures" in order to better understand why GRCs represent a valuable tool. This first part also present two useful documents: a framework created by Forrester to help CEOs in calculating the ROI of an integrated GRC system and the work "Big Picture for Governance, Risk, and Compliance Platforms", created by Politecnico di Milano, focused on the evaluation and classification systems of GRC platforms. This should provide to companies two valuable tools for addressing the phase of project evaluation and GRC vendor selection, in order to choose the solution that better meets their requirements.

The second part is focused on the implementation phase: after presenting the needed prerequisites it provides a list of valuable tips for easing the installation phase and help preventing risks.

Once the implementation phase has been successfully completed the company may be interested in finding some way to continue its improvement process. For this reason the last part of the document is devoted to present two management techniques particularly aligned with the philosophy and modus operandi of the integrated GRC systems. Those are: the BYOD policies (for managing the use of personal devices for business purposes) and the "Just Culture" (regarding the risk management culture and processes).

Key words: GRC, Implementation, Prerequisites, silo structure, BYOD, Just Culture

ABSTRACT (ITALIAN)

Il presente documento riguarda uno studio, di tipo literature review, riguardante i sistemi GRC integrati. Lo scopo è quello di creare un documento, diretto alle aziende interessate ai sistemi GRC integrati, che raccolga e fornisca informazioni utili circa queste piattaforme (le loro caratteristiche, i prerequisiti necessari ed alcuni suggerimenti per la loro implementazione, ecc.).

Questo dovrebbe aiutare le compagnie a selezionare gli argomenti più interessanti per la loro realtà aziendale in modo da poterli approfondire successivamente; allo stesso momento dovrebbe permettere loro di riuscire ad inquadrare tutti gli elementi coinvolti in questo tipo di progetti, in modo da avere una visione completa del problema e facilitare poi le operazioni di project management.

In altre parole, questo documento dovrebbe essere utilizzato nello studio preparatorio, durante il primo approccio tra l'azienda ed i sistemi GRC integrati.

I materiale utilizzato per questo progetto riguarda pubblicazioni di società di consulenza o esperti ed interviste ai CEO di aziende che hanno implementato con successo un sistema GRC integrato e ne fanno un uso continuo e proficuo: ciò permette non solo di avere degli importanti suggerimenti per la fase d'implementazione, ma soprattutto delle testimonianze di quali vantaggi questi strumenti hanno portato alle loro imprese.

La forma e la struttura di questo documento sono state pensate in funzione del pubblico per cui è creato: vi sarà un uso frequente di elenchi per cercare di facilitarne la lettura ed esempi pratici (secondary data o business case) per supportare la trattazione.

Il lavoro complessivo risulta suddiviso in tre parti.

La prima parte riguarda da vicino i sistemi GRC integrati (cosa sono, come agiscono, quali vantaggi possono portare, ecc.) e i problemi delle cosiddette strutture aziendali "a silos", in modo da comprendere meglio perché i GRC vengono considerati degli strumenti preziosi.

In questa prima sezione vengono anche presentati al lettore due utili documenti: un framework creato da Forrester per calcolare il ROI di una piattaforma GRC ed il lavoro "Big Picture for Governance, Risk and Compliance Platforms" focalizzato sui sistemi di valutazione e classificazione delle piattaforme GRC. Ciò dovrebbe fornire alle aziende due importanti strumenti per la fase di valutazione del progetto e di selezione dell'offerta o GRC vendor più adeguati alla propria situazione.

La seconda parte riguarda la fase di implementazione: dopo aver presentato i prerequisiti necessari si passa ai consigli pratici per completare l'installazione in maniera più agevole e poter prevenire alcuni rischi.

Una volta completata con successo l'implementazione, l'azienda potrebbe essere interessata ad identificare e valutare delle occasioni per completare il proprio processo di miglioramento cominciato con l'adozione del nuovo sistema GRC integrato.

Per tale ragione l'ultima parte è dedicata a presentare due tecniche di gestione particolarmente allineate con la filosofia e le pratiche dei sistemi GRC. Esse rappresentano quindi un'opportunità di supportare e completare il nuovo sistema, ed al contempo sfruttare sinergie e affinità per rendere la fase di implementazione particolarmente agevole e vantaggiosa.

Le due tecniche in questione sono: la BYOD policy (Bring Your Own Device: riguarda la gestione e l'utilizzo di personal devices per lo svolgimento di attività lavorative) e la cosiddetta "Just Culture" (riguardante la cultura e i processi di gestione del rischio).

Parole chiave: GRC, Implementazione, Prerequisiti, Strutture a silos, BYOD, Just Culture

ACRONYM USED

ANSV	Agenzia Nazionale per la Sicurezza del Volo
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
GRC	Governance, Risk, and Compliance
ICT	Information and Communication Technology
IT	Information Technology
KPI	Key Performance Indicator
OCEG	Open Compliance and Ethic Group
ORM	Operational Risk Management
ROI	Return On Investment
SCRM	Supply Chain Risk Management
SVM	Sourcing & Vendor Management

EXECUTIVE SUMMARY (ENGLISH)

Over the years, the use of new business management systems called GRC (Governance, Risk and Compliance) has been affirming and spreading.

This document intends to support companies interested in integrated GRC systems by providing all the needed information to properly frame all the elements involved in such a project. In other words this should to be considered as a preparatory work to be used during the first approach to GRC systems, in order to provide ideas that help the reader to focus on what considers more important or appropriate to his business reality.

The material used to create this document comes from publications and interviews to CEOs of companies that have successfully implemented an integrated GRC system and make a continuous and profitable use of it.

This project aims to cover all the phases that a company goes through since the time it discovers the need of adopting an integrated system until it successfully implements it. In order to do so the document has been divided into three main steps:

1. Show the potential of GRC systems as tools to improve business performance and solve some problems typical of a "silo structure".
2. Provide tools and guidelines for the selection and implementation phases so that the company can make these steps in a more conscious way.
3. Provide cues to continue the improvement process and enable the company to make the most of the investment on the new GRC system.

Let's start by clarifying what GRC systems are and how they work.

Their purpose is to reorganize corporate structure and modus operandi to improve their efficiency and effectiveness through a better resource utilization, waste reduction, improved internal communication management, and providing the top manager with a stream of information always complete and updated to support the decision-making process.

This requires, first of all, the creation of a centralized system for gathering, analyzing and storing information that becomes the backbone of the whole enterprise, enabling it to capitalize on the company's knowledge. All departments will need to collaborate by supplying the information system with data coming from their respective fields, allowing better visibility and control, free internal resources used for unnecessary duplication of functions, exploit opportunities and synergies that may have remained hidden.

The next step is to integrate Risk Management and Governance Management in all other operations carried out inside the company. The underlying idea is to consider risk management and regulation as the functions that usually show an inefficient use of corporate resources. Some experts argue that these two processes, despite the fact that they concern all areas of the enterprise, are often carried out in an improvised and unstructured way, all complicated by the fact that communication between departments is often lacking and difficult.

One of the purposes of the GRC is to improve internal communication within the company and to ensure that management of risks and standards are managed in a structured and conscious way, as a homogeneous component of all the other operations; this should ease company management and at the same time effectively protect the organization against risks and their consequences.

As we might already guess, although GRCs can be considered as an IT system, they are actually a new method of managing therefore require to train and involve staff at all levels and at the same time to redesign the structure of the company in order to eliminate the so-called "silo structure".

For these reasons, it is clear that the implementation of an integrated GRC system is very complex and costly under different perspectives, and it is therefore important to share all the information and experiences useful to successfully completing such a project.

For this reason one of the main purposes of this work is to collect material from publications or companies that have successfully adopted an integrated GRC system and provide guidelines for companies that want to tackle such a project.

As a result, has been chosen to adopt a Literature Review structure and a form as straightforward and practical as possible to meet the needs of the readers for which it is created.

Thanks to the testimonies of the CEO of some Italian companies, we can provide some examples of how the company usually discovers the need to adopt an integrated system; this should provide to the reader an opportunity to make a first comparison with the business reality of its company.

In Italy, the first areas that are adopting a GRC system are the Finance sector, mainly concerned in security and risk management, and the Telecommunications sector, mainly concerned in compliance.

In the industrial field, this topic is still relatively new, but we can see an ever-growing interest in GRC systems, mainly linked to the need for greater control and flexibility.

Within a company, usually the sector that firstly shows the need for more structured procedures is the compliance function, which is often carried out in an improvised way, resulting in an inefficient use of resources. In fact, as the level of complexity increases (due to the frequency with which standards are updated, increased number of regulations to which the company adheres, etc.), arises the need to create a more structured system.

Among the various options available, top managers can considers the adoption of an integrated GRC system in order to act on the entire company (rather that meet just the need raised, for example, of compliance function) by creating an integrated system capable to identify and eliminate the root causes of many problems and so bringing great benefits to the whole organization. Once the company (usually the CEO) shows an interest in adopting a GRC system, a formal proposal must be submitted to the board of directors.

For this reason, is presented to the reader framework, created by Forrester, for calculating the ROI of an integrated GRC platform; its aim is to help the CEO in creating a document to be presented to his company's board of directors in order to support the proposal of adopting of an integrated GRC.

The framework suggests articulating the document in three parts:

1. Identifying and quantifying costs (contains an in-depth discussion of how to estimate costs and what alternatives might be available for the top manager).
2. Identifying and quantifying the benefits obtainable; Forrester divides them into three categories: Efficiency, Risk Reduction and Strategic Performance (figure 1). Although the benefits of the first two categories can be easily quantified in terms of saved hours, reduction of management costs or mitigation of the consequences, the "Strategic Performance" group appears to be more difficult to be expressed with quantitative indicators. For this reason, Forrester identifies two types of flexibility: Extensibility of Investment (which guarantees savings in case of future integration of new packages within the GRC system) and Agility In Business Support (which assures advantages in and savings in case of integration with new suppliers, partner or workforce) (figure 2).
3. Project-related risk identification, divided into 4 categories: Unforeseen costs and delays, Resistance to adoption by users, Integration problems with pre-existing IT platforms, and finally what Forrester calls "Vendor Viability". This last category includes the risks that arise when the relationship with a supplier becomes vital for the

success or failure of a product, project or business model. This implies that the company can initially handle “directly” the risk by identifying, for example, the most robust vendors and choose the most proper one for establishing a long-term relationship. The company, however, may not have the chance to perceive the actual risk or vulnerability of its vendor, thus exposing itself to serious risk or consequences in case the vendor should suffer s disruption, as a result of accidents or poor strategic choices.

Category	Examples	Example calculations
Efficiency	<ul style="list-style-type: none"> • Policy and control management (faster development, review, update, approval, distribution, access, and attestation) • Risk management (faster risk identification, analysis, evaluation, and monitoring) • Audit management (improved scoping, scheduling, data collection, and reporting) • Compliance management (easier association of controls, control assessments, assessment data aggregation, and reporting) • Action management (faster event identification, notification, escalation, remediation, review, and approval) 	<ul style="list-style-type: none"> • Hours saved per function multiplied by the average rate for fully burdened risk, compliance, or audit professionals • Payroll savings from delay or avoidance of staff increases • Reduction in costs of external audits and assessments
Risk reduction	<ul style="list-style-type: none"> • Improved compliance (fewer audit findings, regulatory enforcement actions, and lawsuits) • Improved risk treatment (prioritized and faster remediation) • Improved risk posture (lower cost of capital and insurance premiums) 	<ul style="list-style-type: none"> • Reduction in incident response costs • Reduction in the number and size of fines and penalties • Increase in risk exposure mitigated per dollar/hour spent • Reduction in cost of capital • Reduction in insurance premiums
Strategic performance	<ul style="list-style-type: none"> • Greater oversight (fewer unexpected loss events, accurate view of risk and compliance posture) • More informed decisions (related to development, procurement, and investments) • Better performance (more successful product launches, market expansions, branch openings, technology implementations, or partner engagements) 	<ul style="list-style-type: none"> • Reduction in costs required for unexpected, short-term injections of capital, staff, or other resources • Greater amount of relevant data to support decision-making • Increase in financial or on-time performance (business units, partners, projects, etc.)

56677

Source: Forrester Research, Inc.

Figure 1: Types of benefits of an integrated GRC system (Source: Forrester Research, Inc.)

Category	Examples	Example calculations
GRC extension flexibility	<ul style="list-style-type: none"> • Using the platform for multiple GRC domains (i.e., business continuity, IT, environmental, financial, etc.) • Ability to react quickly to new and changing regulations 	<ul style="list-style-type: none"> • Estimated cost savings from platform consolidation (i.e., spending \$30,000 to \$40,000 on the business continuity module of a GRC platform versus \$200,000 to \$400,000 for a standalone business continuity management platform) • Cost to configure GRC platform for new regulatory content versus cost of a new compliance management product
Business agility flexibility	<ul style="list-style-type: none"> • Smoother integration of business partners, acquired entities, new employees, etc. 	<ul style="list-style-type: none"> • Number of hours (or days) of reduced compliance training and ramp-up time multiplied by productive output of new employee, partner, or acquired entity • Reduction in time and costs of compliance/risk due diligence before strategic decisions • Reduction in opportunities missed because of a lack of compliance/ risk insight

56677

Source: Forrester Research, Inc.

Figure 2: Components of "Strategic Performance" (Source: Forrester Research, Inc.)

From this framework, the reader can already have a more precise idea of the practical benefits that his company might get from using these systems and the order of magnitude of the expected costs, thus preparing for a preliminary cost/benefit analysis.

In the final part of this first section is briefly presented the work of the Politecnico di Milano "*Big Picture for Governance, Risk and Compliance Platforms*" created by Andrea Brusa Perona, Ing. Guido Jacopo Luca Micheli and Prof. Enrico Cagno, focused GRC's evaluation and classification systems.

After identifying the strengths and limitations of existing classification systems, the authors have created a new one by collaborating with some GRC vendors and some companies, interested in adopting a GRC or that was already using it.

Their primary purpose was to support companies in choosing a GRC system by identifying the key features that drive the choice of the platform that best suits their needs while at the same time helping the GRC vendor to show the potentialities and peculiarities of their products.

This should provide to the reader the necessary information of the tools required to select the most proper platform.

At this point, to conclude the introduction about integrated GRC systems we can try to better contextualize these tools by looking at the conditions in which they have been developed and which problems they want to solve (issues related to the use of heavy siloed structure).

For this reason, it is useful to address a brief discussion "silo structures", which today represent the most widespread reality in many medium-large enterprises. The first step is to present the needs and the processes that led to the creation of such structures.

Nowadays companies are operating in increasingly complex environments, characterized by multiple sources and types of uncertainties; organizations are therefore interested in easing business management by trying to filter uncertainties, thus creating determined scenario in which conducting operation more smoothly and at the same time tuning the processes to make them as efficient as possible.

In order to do so, the company identifies the so-called "core functions" (what it considers as the main activities that create value in the product, this can be applied to both manufacturing companies and service providers) and to "Protect" them using the other processes in order to manage and filter the uncertainties.

By doing this, core functions can operate in a predictable and stable environment (although this does not correspond to the actual context in which the company operates, characterized by various forms of uncertainty that are then filtered by the other "buffer functions"); this should allow the company to increase its efficiency and reduce costs, all resulting in an increase of profit margin.

The following figure (Figure 3) should help to understand what has just been said; the central rectangle represents the "core functions", the ellipses represent the "bearing functions" and in bold are some examples of uncertainties affecting the company.

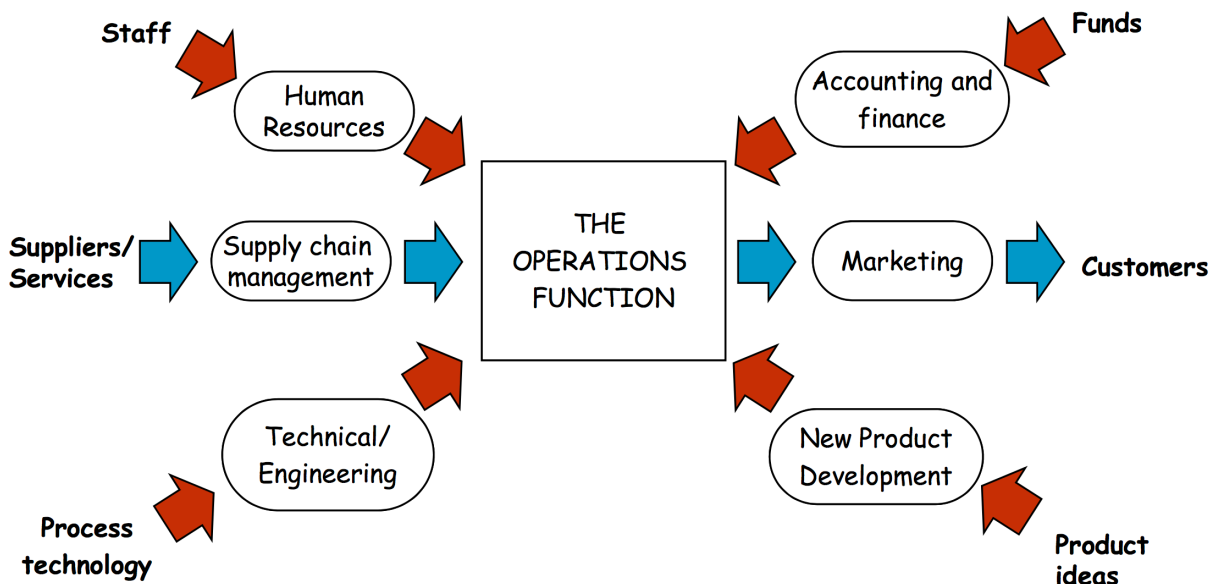


Figure 3: Schematic representation of a "silos structure" (Source: Industrial Risk Management Course)

The main downside is that the various functions work autonomously, each with their own hierarchical structures and local objectives (that might be conflict with each other; a classic example is the management of stock level: the production manager will tend to maintain a high level of stock in order to deal with any unexpected demand fluctuating while stock manager will be interested in keeping stock volume as low as possible in order to contain management costs).

The first consequence of conflicting goals is the use of resources for processes that act in opposition, not only causing a loss of efficiency but sometimes also a loss of effectiveness, resulting from failure to properly manage the problem in order to find the optimal trade-off condition.

The factor that further complicates this situation is the inadequate management of internal communication, which can lead to two types of problems.

We can define the first one as "lack of vertical communication" in which top management has a poor visibility of the organization reducing the awareness of what resources the company has and where they have been allocated, resulting in an increased difficulty to assign local goals and track their progress (all this may lead to situations like the one with conflicting objectives that we have described earlier).

We can define the second one as the "lack of horizontal communication" in which we have delays and missing communications between departments that create circumstances in which problems develop unnoticed, thus hampering risk management processes in all their phases (identification, analysis, mitigation, control).

In some business realities, we can see some "extreme" situation where risk and compliance management roles are seen as the figures that try to "put the brake on" strategic business decisions, and therefore are not included in that process.

This is for sure one of the biggest mistakes an organization could make because compliance and risk management functions are the most important capable of identifying all the implications and relevant factors involved in the decision that the company is evaluating, thus enabling the decision-making process to take strategic and conscious choices, improving the chance that they will prove successful.

Among the examples included in this section there is also the "Mattel case" of 2007, in order to allow the reader to better understand the magnitude of possible consequences arising from a loss of visibility and monitoring.

The importance of this overview about "silo structure" and its problems allows the reader to understand the needs that led to the development and use of GRCs, which entrust to internal communication management a key role in allowing the company to operate efficiently and affectively in very complex environment, having better awareness of its potential, internal and external risks and implemented protections.

The next step is to identify the requirements needed for a successful implementation.

As we pointed out at the beginning of this document, GRCs require an evolution of both the corporate structure and all the staff so, in order to support the company in enduring the effort, it is necessary to have the convinced and total support of high management combined with a certain level of business maturity.

This latter concept mainly concerns risk management culture and procedures used by the organization and so has been identified some concepts capable of assessing the "maturity level" of the company.

The requirements identified consulting the publication of experts and managers are listed:

1. Own and use a consolidated risk management system.
2. Conduct proactive risk management.
3. Be aware that operational risk can be both a threat or a opportunity;
4. Know the importance of corporate resilience, how to build it, and its value in a proactive view.

Point 1 can be considered as the real essential requirement for attempting the implementation, however, points 2 to 4 are important to be able to use more properly the new integrated GRC systems and to take full advantage of its potential, enabling the company to fully exploit the investment and to achieve the benefits mentioned in this document.

To support the discussion of this section and to give to the reader a testimony of the potential and benefits of proactive risk management how operational risk (looking like a threat) can be transformed into an opportunity, is presented in the Nokia-Ericsson case of 2000.

At this point are provided some "practical tips" for managing GRC's implementation by presenting a collection of successful procedures for a smooth and conscious implementation.

The material used to create these best practices comes primarily from interviews issued by CEOs of companies that have successfully implemented a GRC platform and are making a continuous and profitable use of it, and can therefore appreciate and testify the benefits it has brought to their organization.

We can now list these the suggested procedures:

1. Being able to communicate the reasons for the adoption of a GRC system and motivate the staff. This point basically consist on motivating the staff to participate in the implementation of the new system, but also to effectively use the system when normal operating conditions will be restored. In fact the way and the extent in which workers interact with the new system will substantially decrees the success (correct and continuous use of the system) or failure (creation of different and "illegal" communication channels, thus losing the flow of information on which GRCs are based all its processes) of the project/investment;
2. Creating a common vocabulary in all sectors of the company. In fact it may happen that different departments use the same word with two different meanings, making it necessary to create a common language for all the corporate function that now have to

communicate and cooperate in feeding the new centralized information management system;

3. Training the staff (ideally of the all, but in practice is enough to select just the workers in charge of interacting with the information system) about the fundamentals of risk management (and maybe also regulatory management if it is particularly important for the business of the company) in order to make them able to recognize all the useful information and be aware of their value, thus potentially increasing the amount of data collected and processed;
4. Active staff involvement in creating the structure of audits and forms for data entry; This should makes the staff feel more involved and motivated to use a system that has helped to create rather than seeing it "imposed" from the top; at the same time this should prevents the risk of creating a difficult and uncomfortable system interface, thus avoiding the problems identified in point 1;
5. Step-by-step project management: some CEOs suggest conducting the implementation in small steps. In fact as we said this process involves the entire organization but having limited resources and the need to maintain business continuity, the best approach seems to be to take one department at the time and integrate it into the new system (software / hardware implementation and staff training) and then move on to the next one, creating step by step the final form.

Once the implementation phase has been successfully completed and the organization has restored the normal operating conditions, the company may be interested in finding some tools or management techniques to continue the improvement process begun with the adoption of an integrated GRC system.

For this reason the last part is devoted to present two management techniques particularly in line with GRC's philosophy and procedures, and may therefore represent an interesting and easily way of integrating and complementing the new system taking advantage of some synergies.

The two methodologies are: the BYOD policy and the so-called "Just Culture".

BYOD policy deals with the use of personal devices for business purposes with the aim of increasing productivity while maintaining an adequate level of security and data protection. This subject is particularly delicate and carries some difficulties; for this reason, over the years, several initiatives have taken place: BYOP (Bring Your Own PC), Bring Your Own Phone (BYOP), BYO (Bring Your Own Devices), BYOD (Bring Your Own Devices), presenting an increasingly difficult challenge for IT Security, which today needs to develop security solutions while dealing with a large number of products (smartphones, computers, tablets, OSs, etc.) and versions (different brands, operating system), that change with a dizzying rhythm.

For this reason, the BYOD has been used in this document to present the entire set of different management techniques, focusing just on 3 of them: MAM (Mobile Application Management), Mobile Device Management (MDM) and MEM (Mobile Expense Management).

We can expect that the use of personal devices could bring great benefits to GRCs by motivating staff to use their own devices (with whom they are more confident) to interact with the central information management system in a more comfortable, quick and frequent way, and therefore we can expect an increase in the amount of data collected and analyzed.

"Just Culture" is born in the aeronautics field (in particular with regard to air traffic security management) and concerns the creation of a business culture centered on proactive risk management.

The discussion begins providing an extract from the article "Trasporto aereo. Imparare dagli errori. Ecco cos'è la just culture" (In English: "Air Transport. Learn From Errors. Here is

the Just Culture”) by Patrizio Paolinelli (Wordpress) to show how it is particularly important to create the risk management system over an “healthy” risk culture. In addition it tries to explain why would be so important to bring this (Anglo-Saxon) mentality into our country, in order to finally contribute to the cultural change necessary for creating a proactive and proficient risk management system capable of guarantee an adequate level of protection in particularly complex environments such as aeronautical (and some industrial field such as: power plants, oil platforms, state-of-the-art facilities, etc.).

These techniques also allow organizations to reach high levels of protection and risk prevention in many areas, thus responding to the increasingly widespread need for proactive risk management.

“Just Culture” requires first of all the creation of structured procedures for risk management through a common effort and collaboration of all the hierarchical levels of the company, all supported by the regulations and other useful resources.

Is very important that risk management processes are built over a risk culture capable of identify its priorities and objective (its only concern has to be risk prevention/protection, any other goal would just reduce its performances), knowing all the tools that might be useful to perform its tasks and also knowing the value and potential of prevention and asset reliability. This is more or less what we have highlighted as requirements for a successful use of a GRC system, so we can find a first sign of the fact that “Just Culture” and GRC’s risk component are well aligned.

The second step requires the creation of a system for collecting and analyzing safety data defined as “voluntary reports”, usually they are minor events (minor failures or minor anomalies found during operations or maintenance or the so-called “near misses”, events that could result in accidents but were interrupted before they could bring serious consequences) that the legislation considers non-mandatory.

These data are extremely valuable in fact particularly complex systems (in which we may have different actors, procedures, systems interweaving and collaborating) because it is practically impossible to predict all the possible situations in which an accident may occur. These reports can highlight criticalities that under certain conditions could lead to serious consequences.

We therefore understand that we are dealing with a real treasure of information, which could also help, for example, in health and safety operations and asset protection (basically systems reliability).

However, in order to establish this information gathering system the organization has to create a mutual trust relationship between the various levels of the company.

In fact, although these data are entered in the system following precise procedures to protect the privacy of the people involved (personal information are removed, but general information are used to classify and analyze the event; for examples the report describing for example the role of the people involved: e.g.: pilot, mechanic, etc.; the type of system: airplane X, machine Y, etc.), it may be still possible to identify the people mentioned.

For example, if we consider a small airline in which only two pilots are trained and assigned to pilot aircraft XY or a small company where there is only one milling machine. We understand that if the report is about a “near miss” event happened to the aircraft XY or a milling machine, it would be straightforward to trace who might have committed and “anonymously confessed” the mistake.

It is therefore extremely important that, except case of abuse, malicious intent or serious negligence attributable to an individual who will be properly prosecuted, these reports are used exclusively for risk management purposes and never to identify and prosecute the persons involved except for the aforementioned cases.

Here we get reconnect to what has been said before: in our country would be extremely important to bring a mentality of this type, capable of understanding that the pursuit of scapegoat is not useful to anyone, while a management like the one just presented does not aim to leave the guilty walk free for the sake of safety, but is able to attribute responsibilities to all the people involved and at the same time to contribute actively to the prevention of accidents.

We may expect that “Just Culture” could bring several benefits to the company's GRC system, first of all by completing and supporting its risk management culture (Risk function) that consider proactive risk management a priority.

Secondly, the collection and analysis of voluntary reports could not only bring benefits to risk management and compliance functions, but it may also encourage staff to contribute actively by reporting any particular event and thus increasing the awareness and responsiveness of the entire organization potentially in any area.

This represent the conclusion of the present work, we hope that it can prove useful serving as a consultation document for companies interested in GRCs and providing the necessary insights to deepen the various themes and contribute to reach a successful and profitable implementation of these systems.

We also hope that this document will become the starting and contact point for a set of successive works each one focused on one of the different themes addressed here in a superficial way.

Among the topics that seem to be more interesting and less tackled today, we think that the identification and analysis of management techniques (such the two we just mentioned) particularly aligned with GRC systems, could be very useful to discover and spread interesting opportunities for completing and enriching these valuable integrated systems.

EXECUTIVE SUMMARY (ITALIAN)

In questi anni si sta affermando e diffondendo l'utilizzo di nuovi sistemi per la gestione aziendale denominati GRC (Governance, Risk and Compliance).

Questo documento intende supportare le aziende interessate ai sistemi GRC integrati mettendo a disposizione le conoscenze reperibili da pubblicazioni ed interviste a CEO di aziende che hanno implementato con successo un sistema di questo tipo e ne fanno un uso continuativo nel tempo.

Lo scopo primario di questo progetto è quello di creare un'opera riassuntiva in grado di aiutare le aziende ad individuare e prendere coscienza di tutti gli elementi che entrano in gioco quando dal momento in cui un'impresa manifesta interesse nell'adozione di un sistema GRC integrato. In altre parole questo documento dovrebbe essere utilizzato nelle fasi iniziali, in cui un'azienda cerca di capire meglio sia cosa i GRC possono portare alla propria realtà lavorativa sia quali possano essere i requisiti necessari, non solo per un'implementazione di successo, ma anche per creare le condizioni adatte ad un utilizzo completo e redditizio.

Si cercherà quindi di fornire importanti spunti di approfondimento ai lettori in modo che possano concentrarsi su quello che ritengono più importante o adatto alla loro realtà aziendale e compiere in maniera più consapevole i passaggi principali, come la selezione dei fornitori e l'implementazione vera e propria del nuovo sistema.

Questo progetto intende coprire tutte le fasi che un'azienda attraversa da quando si scopre interessata ad un sistema integrato fino a quando lo implementa con successo.

Il documento si pone 3 obiettivi principali:

1. Mostrare le potenzialità dei sistemi GRC come strumenti per migliorare le performance aziendali e risolvere alcuni problemi tipici di una struttura a "silos";
2. Fornire degli strumenti e linee guida per la fase di selezione ed implementazione in modo da poter compiere in maniera più consapevole questi passaggi;
3. Fornire spunti per proseguire il processo di miglioramento continuo e permettere all'azienda di sfruttare al massimo l'investimento compiuto sul nuovo sistema GRC.

Cominciamo col chiarire meglio cosa sono i sistemi GRC e come agiscono.

Il loro scopo è quello di riorganizzare la struttura ed il modus operandi aziendale per migliorarne l'efficacia e l'efficienza tramite un utilizzo migliore delle risorse, l'eliminazione di sprechi (duplicazioni di processi non necessarie), una migliore gestione della comunicazione interna e fornendo al top manager un flusso informativo sempre completo ed aggiornato per supportare il processo decisionale dell'azienda.

Ciò richiede innanzitutto la creazione di un sistema centralizzato di raccolta, analisi e immagazzinamento delle informazioni che diverrà di fatto la spina dorsale della nuova struttura aziendale, permettendo all'organizzazione di capitalizzare al meglio la propria Knowledge.

Tutti i dipartimenti aziendali dovranno quindi collaborare alimentando il sistema informativo con informazioni provenienti dai loro rispettivi campi, permettendo così all'azienda di avere una migliore visibilità e controllo delle risorse impiegate, al fine di eliminare inutili duplicazioni di funzioni e sfruttare opportunità e sinergie di cui poteva non essere a conoscenza.

Il passo successivo è quello di prendere le funzioni di gestione del rischio (Risk) e gestione degli adeguamenti normativi (Governance) e renderle parte integrante di tutte le operazioni svolte in azienda.

L'idea che sta alla base è quella di considerare la gestione del rischio e quella normativa come le funzioni che solitamente mostrano un utilizzo non efficiente delle risorse aziendali.

Alcuni esperti sostengono infatti che questi due processi, nonostante tocchino tutti gli ambiti dell'impresa, vengano spesso condotti in maniera estemporanea e non strutturata, il tutto complicato dal fatto che la comunicazione tra i dipartimenti risulta spesso carente e difficoltosa.

Uno degli scopi dei GRC è appunto quello di migliorare la comunicazione interna dell'azienda e far sì che la gestione del rischio e delle norme venga condotta in maniera strutturata e consapevole, come una componente omogenea in tutte le operazioni, permettendo così all'impresa di compiere una migliore gestione e nel contempo proteggersi più efficacemente dai rischi e dalle loro conseguenze.

Come già si potrebbe intuire, sebbene i GRC si presentino come dei sistemi informatici, essi sono in realtà un nuovo metodo di gestione a tutti gli effetti e come tale richiedono un grande lavoro di formazione e coinvolgimento del personale a tutti i livelli unito ad una riprogettazione della struttura aziendale (superamento della struttura definita "a silos").

Per questi motivi risulta evidente che l'implementazione di un sistema GRC integrato risulterà molto complessa e costosa sotto diversi punti di vista; diventa quindi importante condividere tutte le informazioni e le esperienze utili a completare con successo un progetto di questo genere.

Il presente lavoro nasce proprio con l'obiettivo di raccogliere materiale proveniente da pubblicazioni di esperti o esperienze di aziende che hanno adottato con successo un sistema GRC integrato per poter quindi fornire delle linee guida alle imprese che intendono affrontare un simile progetto.

Di conseguenza si è scelto di adottare una struttura Literature Review ed una forma il più possibile diretta e pratica per venire in contro alle esigenze del pubblico per cui è pensato.

Grazie alle testimonianze di alcuni top manager italiani, vengono riportati alcuni esempi di come solitamente nasce in azienda il bisogno di ricorrere all'utilizzo di un sistema integrato e strutturato, per poter fornire al lettore alcune occasioni di confronto col la propria realtà aziendale.

In Italia gli ambienti che per primi si stanno aprendo all'adozione di un sistema GRC sono il settore Finance, interessato soprattutto alla sicurezza e alla gestione dei rischi, e quello delle Telecomunicazioni maggiormente interessato all'aspetto della compliance.

In campo industriale l'argomento è ancora relativamente nuovo ma si percepisce una spinta in tale direzione legata soprattutto ad un'esigenza di maggiore controllo e flessibilità.

All'interno delle aziende, il settore da cui più frequentemente nasce un tale bisogno è quello riguardante la gestione normativa, la quale viene spesso condotta in maniera destrutturata determinando perciò un utilizzo di risorse non efficiente; mano a mano che il livello di complessità aumenta (frequenza con cui si aggiornano le norme, aumento del numero di normative a cui l'azienda aderisce, ecc.) nasce quindi la necessità di ricorrere alla creazione di un sistema strutturato, ordinato e più facilmente controllabile.

Tra le varie opzioni a disposizione del top manager si trovano proprio i GRC che permettono di sfruttare l'opportunità offerta dal dover rispondere ad un'esigenza specifica (come quella appena mostrata) per decidere invece di agire a livello dell'intera azienda, creando un sistema integrato capace di identificare e gestire le cause profonde responsabili di diversi problemi e portare così grandi benefici all'intera impresa.

Una volta che l'azienda (solitamente il CEO) riscontra un bisogno/interesse nell'adozione di un sistema GRC dovrà essere creata una proposta da sottoporre al consiglio di amministrazione.

Per questa ragione viene presentato al lettore il framework di Forrester per il calcolo del ROI di una piattaforma GRC integrata; esso ha lo scopo di aiutare il CEO nella creazione del documento da presentare al consiglio di amministrazione della sua azienda per supportare la richiesta di adozione di un GRC integrato.

Il framework suggerisce di articolare il documento in tre parti:

1. Individuazione e quantificazione dei costi (viene fornita una trattazione approfondita di come stimare i costi e quali alternative il top manager potrebbe avere a disposizione);
2. Individuazione e quantificazione dei vantaggi ottenibili, Forrester li suddivide in 3 categorie: Efficiency, Risk Reduction e Strategic Performance (figura 1). Sebbene i vantaggi offerti dalle prime due categorie possano essere facilmente quantificati in termini di ore-uomo risparmiate, riduzione dei costi di gestione o mitigazione delle conseguenze, il gruppo "Strategic Performance" appare più difficile da rappresentare con indicatori quantitativi. Per tale ragione Forrester identifica due tipi di flessibilità: GRC extension flexibility (che garantisce risparmi nel caso si intenda integrare, in futuro, nuovi pacchetti all'interno del sistema GRC) e la Business agility flexibility (che garantisce risparmi di risorse in vari tipi di operazioni commerciali come la fusione con un partner) (figura2);
3. Identificazione dei rischi legati al progetto, suddivisi in 4 categorie: costi e ritardi dovuti ad imprevisti, resistenza all'adozione da parte degli utenti, problemi di integrazione con piattaforme IT preesistenti ed infine quella che Forrester definisce "Vendor Viability". Quest'ultima categoria comprende i rischi a cui ci si espone quando si affida al rapporto col proprio fornitore un'importanza vitale per la riuscita o il fallimento di un prodotto, progetto o business model. Ciò implica che l'azienda può inizialmente gestire il rischio in maniera diretta identificando ad esempio il vendor con il profilo più solido e che garantisce maggiori probabilità di poter mantenere un rapporto duraturo nel tempo; l'azienda potrebbe tuttavia non avere la possibilità di percepire la reale inclinazione al rischio o le vulnerabilità del proprio fornitore esponendosi così al rischio di trovarsi senza supporto nel caso il vendor subisca l'interruzione delle attività a seguito di incidenti o scelte strategiche sbagliate.

Category	Examples	Example calculations
Efficiency	<ul style="list-style-type: none"> • Policy and control management (faster development, review, update, approval, distribution, access, and attestation) • Risk management (faster risk identification, analysis, evaluation, and monitoring) • Audit management (improved scoping, scheduling, data collection, and reporting) • Compliance management (easier association of controls, control assessments, assessment data aggregation, and reporting) • Action management (faster event identification, notification, escalation, remediation, review, and approval) 	<ul style="list-style-type: none"> • Hours saved per function multiplied by the average rate for fully burdened risk, compliance, or audit professionals • Payroll savings from delay or avoidance of staff increases • Reduction in costs of external audits and assessments
Risk reduction	<ul style="list-style-type: none"> • Improved compliance (fewer audit findings, regulatory enforcement actions, and lawsuits) • Improved risk treatment (prioritized and faster remediation) • Improved risk posture (lower cost of capital and insurance premiums) 	<ul style="list-style-type: none"> • Reduction in incident response costs • Reduction in the number and size of fines and penalties • Increase in risk exposure mitigated per dollar/hour spent • Reduction in cost of capital • Reduction in insurance premiums
Strategic performance	<ul style="list-style-type: none"> • Greater oversight (fewer unexpected loss events, accurate view of risk and compliance posture) • More informed decisions (related to development, procurement, and investments) • Better performance (more successful product launches, market expansions, branch openings, technology implementations, or partner engagements) 	<ul style="list-style-type: none"> • Reduction in costs required for unexpected, short-term injections of capital, staff, or other resources • Greater amount of relevant data to support decision-making • Increase in financial or on-time performance (business units, partners, projects, etc.)

56677

Source: Forrester Research, Inc.

Figura 1: Esempi di vantaggi divisi in 3 categorie: Efficiency, Risk Reduction e Strategic Performance (Fonte: Forrester Research)

Category	Examples	Example calculations
GRC extension flexibility	<ul style="list-style-type: none"> • Using the platform for multiple GRC domains (i.e., business continuity, IT, environmental, financial, etc.) • Ability to react quickly to new and changing regulations 	<ul style="list-style-type: none"> • Estimated cost savings from platform consolidation (i.e., spending \$30,000 to \$40,000 on the business continuity module of a GRC platform versus \$200,000 to \$400,000 for a standalone business continuity management platform) • Cost to configure GRC platform for new regulatory content versus cost of a new compliance management product
Business agility flexibility	<ul style="list-style-type: none"> • Smoother integration of business partners, acquired entities, new employees, etc. 	<ul style="list-style-type: none"> • Number of hours (or days) of reduced compliance training and ramp-up time multiplied by productive output of new employee, partner, or acquired entity • Reduction in time and costs of compliance/risk due diligence before strategic decisions • Reduction in opportunities missed because of a lack of compliance/risk insight

56677

Source: Forrester Research, Inc.

Figura 2: Esempi di strategic performance considerando due tipi di flessibilità (Fonte: Forrester Research)

Da ciò il lettore potrebbe già farsi un'idea più precisa dei vantaggi pratici che la sua azienda potrebbe ottenere dall'utilizzo di questi sistemi e dell'ordine di grandezza dei costi previsti, potendo così elaborare ad un'analisi costi/benefici preliminare.

Nella parte finale di questa prima sezione del documento viene presentato brevemente il lavoro *“Big Picture for Governance, Risk and Compliance Platforms”* del Politecnico di Milano ad opera di Andrea Brusa Perona, Ing. Guido Jacopo Luca Micheli e Prof. Enrico Cagno che analizza i sistemi esistenti di classificazione delle piattaforme GRC.

Gli autori, dopo aver identificato i punti di forza e le limitazioni dei sistemi di classificazione esistenti, ne hanno elaborato uno nuovo collaborando con alcuni GRC vendor e alcune aziende interessate ad adottare un GRC o che già ne facevano uso.

Il loro scopo primario era infatti quello di supportare le aziende nella scelta di un sistema GRC identificando le caratteristiche principali che guidano la scelta della piattaforma più adatta alle proprie esigenze e contemporaneamente aiutando i GRC vendor a mettere in mostra le potenzialità e le peculiarità dei propri prodotti.

Questo dovrebbe fornire alle aziende interessate le informazioni necessarie a conoscere gli strumenti che la possano aiutare nella selezione della piattaforma GRC più adatta alle proprie esigenze, utilizzando uno o più dei sistemi di classificazione disponibili.

A questo punto si può considerare conclusa l'introduzione ai sistemi GRC integrati, avendone mostrato le potenzialità ed alcuni strumenti per valutarne l'applicabilità alla propria realtà aziendale.

Come risulta ormai chiaro i sistemi GRC nascono per rispondere ad alcune esigenze piuttosto precise, ma riuscire a contestualizzare meglio l'ambito in cui sono stati sviluppati può contribuire ad averne una maggiore comprensione.

Per tale ragione è utile affrontare una breve trattazione circa la struttura aziendale definita “a silos”, che rappresenta ad oggi la realtà più diffusa in molte medie-grandi aziende.

Il primo passo è quello di presentare le esigenze che portarono alla creazione di strutture di questo tipo.

Le aziende si trovano ad operare in ambienti sempre più complessi e caratterizzati da molteplici fonti e tipologie di incertezze; le imprese cercarono quindi di alleggerire la gestione aziendale cercando di filtrare le incertezze creando così uno scenario determinato in cui poter lavorare in condizioni il più possibile stabili, affinando i processi per renderli il più efficienti possibile.

Per fare ciò l'azienda identifica tra le funzioni svolte le cosiddette “core functions” (quelle che l'azienda considera come le principali attività che creano valore nel prodotto, ciò vale sia per le imprese produttive sia per i fornitori di servizi) e le “protegge” utilizzando le altre per gestire e filtrare le incertezze.

Così facendo le “core functions” possono operare in un ambiente determinato e prevedibile (anche se ciò non corrisponde al contesto reale in cui opera l'azienda, caratterizzato invece da varie forme di incertezza opportunamente filtrate dalle altre “funzioni cuscinetto”) in modo da renderle il più efficiente possibile e permettere una riduzione dei costi e un conseguente aumento del margine di guadagno.

Nella figura seguente (figura 3) si può vedere un esempio di struttura “a silos”: il rettangolo centrale rappresenta le “core functions”, gli ellissi rappresentano le “funzioni cuscinetto” e in grassetto sono riportate alcuni esempi di incertezze che impattano l'azienda.

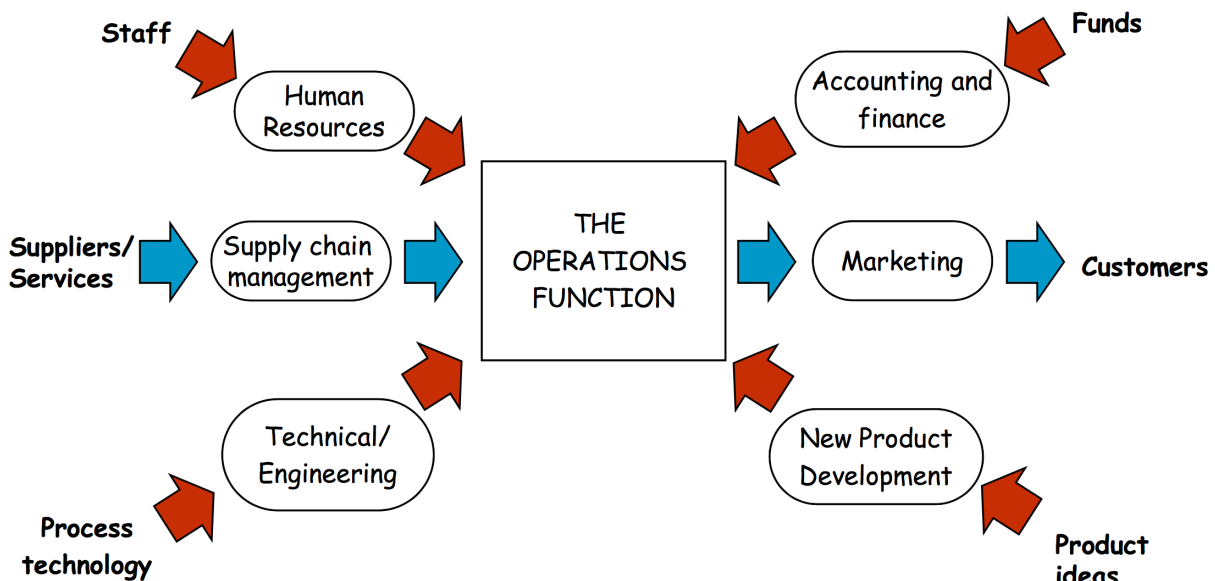


Figura 3: Esempio di struttura aziendale definita "a silos" (Fonte: Corso di Industrial Risk Management)

Il rovescio della medaglia sta nel fatto che le varie funzioni si trovano ad operare in maniera autonoma, ognuna con le proprie strutture gerarchiche ed obiettivi locali che potrebbero risultare contrastanti gli uni con gli altri (esempio classico è rappresentato dalla gestione del livello di scorte a magazzino, siano esse materie prime, semilavorati o prodotti finiti: il responsabile della produzione tenderà a mantenere un alto livello di scorte per fare fronte ad eventuali imprevisti o fluttuazioni della domanda mentre il responsabile di magazzino sarà interessato a mantenere il volume delle scorte il più basso possibile per contenere i costi di gestione).

La prima conseguenza di obiettivi contrastanti è senza dubbio un impiego di risorse che agiscono in opposizione, determinando non solo una perdita di efficienza ma a volte anche una perdita di efficacia derivante dal fatto che, se non si riesce a considerare il problema da un punto di vista più distaccato, non sarà possibile gestirlo in maniera adeguata (trovare un trade-off ottimale tra le due posizioni).

Il fattore che complica ulteriormente le cose è la gestione delle comunicazioni tra i vari dipartimenti: ritardi e comunicazioni non pervenute creano infatti delle circostanze che possiamo dividere in due categorie.

La prima categoria possiamo definirla "mancanza di comunicazione verticale" in cui il medio ed alto management non riesce ad avere una buona visibilità di come vengono svolte le operazioni dei vari dipartimenti;. Ciò comporta una serie di difficoltà come ad esempio nell'identificare e allocare le proprie risorse (rischio di obiettivi risorse che operano in opposizione) o nell'assegnare gli obiettivi locali e tracciarne i progressi (rischio di obiettivi contrastanti o non allineati con gli obiettivi globali dell'azienda).

La seconda categoria può essere definita "mancanza di comunicazione orizzontale", in cui ritardi e mancate comunicazioni creano delle condizioni in cui i problemi e i rischi si sviluppano inosservati e si può perdere la prontezza di identificare, valutare e compiere eventuali misure correttive.

In alcune realtà aziendali si arriva alla situazione estrema in cui le funzioni di gestione dei rischi e delle normative vengono viste come delle figure che "frenano" l'azienda quando c'è da compiere delle scelte strategiche, non capendo invece che l'unico modo per fare scelte consapevoli è utilizzare questi processi per identificare tutti i fattori rilevanti e poter quindi aumentare le possibilità di compiere scelte consapevoli e vincenti.

Tra gli esempi inseriti in questa sezione compare anche il caso Mattel del 2007, al fine di permettere al lettore identificare meglio le possibili conseguenze che nascono da problemi di

comunicazione e visibilità, potendo eventualmente ritrovare alcuni dei problemi già vissuti nella propria realtà aziendale ed avere quindi un ulteriore riscontro del fatto se sia sensato o meno per la sua organizzazione prendere in considerazione l'utilizzo di una piattaforma di questo tipo.

L'importanza di questa panoramica circa la struttura "a silos" e le sue problematiche permette al lettore di capire quali sono le esigenze che hanno portato alla nascita e all'utilizzo dei GRC, i quali affidano alla gestione del flusso informativo interno un ruolo chiave nel permettere all'azienda di operare in maniera efficiente ed efficace, avendo una migliore consapevolezza delle proprie potenzialità, dei rischi (interni ed esterni) e delle protezioni implementate.

Il passo successivo riguarda l'individuazione dei requisiti necessari ad un'implementazione di successo.

Come abbiamo sottolineato all'inizio di questo documento i GRC richiedono un'evoluzione sia della struttura aziendale sia del personale interno e per permettere all'azienda di sopportare lo sforzo è necessario il convinto e totale supporto dell'alto management unito ad un certo livello di maturità aziendale.

Quest'ultimo concetto riguarda soprattutto il sistema e la cultura di gestione del rischio operativo utilizzata dall'azienda e vengono presentati alcuni concetti capaci di "misurare" la maturità dell'impresa.

I requisiti identificati grazie anche al materiale di alcuni esperti e manager che hanno implementato con successo un GRC sono:

1. Possedere ed UTILIZZARE un sistema di gestione del rischio consolidato;
2. Condurre una gestione proattiva dei rischi;
3. Essere consapevole del fatto che il rischio operativo può essere sia una minaccia sia un'opportunità;
4. Conoscere l'importanza della resilienza aziendale, come costruirla, ed il suo valore in ottica proattiva.

Il punto 1 può essere considerato il vero requisito essenziale per tentare l'implementazione, tuttavia i punti da 2 a 4 sono importanti per poter utilizzare in maniera più corretta i sistemi GRC integrati e poterne sfruttare appieno le potenzialità, permettendo all'impresa di far fruttare l'investimento e poter raggiungere i vantaggi accennati in questo documento.

Per supportare la trattazione di questa sezione, dare un'idea concreta al lettore dei vantaggi derivanti da una gestione proattiva del rischio ed una testimonianza di come sia possibile trasformare un rischio in un'opportunità, viene presentato il caso Nokia-Ericsson del 2000.

A questo punto si può passare a parlare dei "consigli pratici" per la gestione dell'implementazione di un GRC presentando una raccolta di procedure rivelatesi vincenti per un'implementazione il più possibile agevole e priva di imprevisti.

Il materiale utilizzato per la creazione di queste best practice proviene principalmente da interviste rilasciate da CEO di aziende che hanno implementato con successo una piattaforma GRC e ne fanno un utilizzo continuativo, potendo quindi apprezzare e testimoniare i vantaggi che ciò ha portato alla loro realtà aziendale.

Di seguito viene riportato l'elenco dei suggerimenti offerti:

1. Riuscire a trasmettere le motivazioni dell'adozione del sistema GRC e quali vantaggi può portare all'azienda e al lavoro del personale. Questo punto riguarda sostanzialmente la motivazione del personale dell'azienda che dovrà non solo partecipare all'implementazione del nuovo sistema, ma sarà anche colui che interagirà

maggiormente con esso, decretando così sostanzialmente il successo (utilizzo corretto e continuativo del sistema) o il fallimento (creazione di canali di comunicazione differenti, facendo così perdere al sistema GRC il flusso di informazioni su cui sostanzialmente si basano tutti i suoi processi) dell'investimento;

2. Creazione di un vocabolario comune a tutti i settori dell'azienda (può capitare infatti che dipartimenti differenti utilizzino lo stesso vocabolo con due significati diversi, rendendo quindi necessaria la creazione ed adozione di un linguaggio comune a tutti);
3. Formazione del personale (idealmente di tutto il personale, ma in pratica è sufficiente il personale incaricato di alimentare il sistema informativo) circa la gestione del rischio (ed eventualmente anche della gestione normativa se risulta particolarmente importante per il business dell'azienda), con lo scopo di far sì che possa riconoscere le informazioni utili e il loro valore, incrementando le potenzialità del processo di raccolta ed analisi dei dati;
4. Partecipazione attiva del personale alla creazione della struttura degli audit e dei form per l'inserimento di dati a sistema; ciò fa sì che il personale si senta coinvolto e più motivato ad utilizzare un sistema che lui stesso ha contribuito a creare piuttosto che vederselo imporre dall'alto; allo stesso tempo previene il rischio di creare un sistema difficile e scomodo da utilizzare, evitando quindi di ricadere nella situazione di "fallimento dell'investimento" che avevamo identificato nel punto 1;
5. Gestione del progetto in fasi: l'implementazione di un sistema GRC integrato coinvolge l'intera azienda ma, essendo le risorse a disposizione limitate ed avendo la necessità di mantenere la continuità del business, l'approccio migliore sembra essere quello di procedere un settore per volta, integrandolo nel nuovo sistema (implementazione software/hardware e formazione del personale) e passando poi al successivo, per giungere passo dopo passo alla creazione della forma finale.

Una volta conclusa con successo la fase di implementazione e raggiunta la condizione di regime si può considerare l'adozione del sistema GRC integrato come il primo passo, compiuto dall'azienda, di un processo evolutivo verso una sempre migliore ed avanzata gestione.

L'ultima parte ha perciò lo scopo di fornire degli spunti per continuare il processo di sviluppo e miglioramento presentando due tecniche di gestione particolarmente in linea con la filosofia e le procedure dei GRC, che potrebbero quindi risultare interessanti per il lettore e facilmente integrabili nel nuovo sistema.

Le due metodologie sono: la BYOD policy e la cosiddetta "Just Culture".

La BYOD policy riguarda l'utilizzo di personal devices per lo svolgimento di alcune attività lavorative con lo scopo di aumentare la produttività mantenendo contemporaneamente un adeguato livello di sicurezza e protezione.

L'argomento è particolarmente delicato e negli anni ha subito grandi modificazioni e miglioramenti; negli anni si sono infatti succedute diverse iniziative: BYOPC (Bring Your Own PC), BYOP (Bring Your Own Phone), BYOT (Bring Your Own Technology), BYOD (Bring Your Own Devices), rappresentando una sfida sempre più difficile per la IT security, che oggi deve elaborare soluzioni di protezione e sicurezza informatica scontrandosi con un grande numero di prodotti (per tipo: smartphone, computer, tablet; per OS; ecc.) e di versioni (sistemi operativi) che cambiano con un ritmo vertiginoso.

Per tale ragione si riporta l'iniziativa BYOD per introdurre la presentazione delle tecniche gestionali che stanno alla base: MAM (Mobile Application Management), MDM (Mobile Device Management) ed MEM (Mobile Expense Management).

Ci si può aspettare che l'utilizzo di personal devices potrebbe portare grandi vantaggi al sistema informativo dei GRC motivando il personale ad utilizzare i propri dispositivi (con cui

hanno grande dimestichezza) per interagire col sistema centrale in maniera più comoda, rapida e frequente; ci si può aspettare quindi un conseguente aumento della quantità di dati in ingresso.

La “Just Culture” nasce in ambito aeronautico (per la gestione della sicurezza del trasporto aereo) e riguarda la creazione di una cultura aziendale incentrata sulla gestione proattiva del rischio che permetta di svolgere le funzioni di risk management in maniera più consapevole ed efficace.

La trattazione si apre presentando un estratto dell’articolo “Trasporto aereo. Imparare dagli errori. Ecco cos’è la just culture” di Patrizio Paolinelli (Wordpress). Ciò aiuta a mostrare come sia particolarmente costruire il sistema di gestione del rischio sopra una risk culture “sana”, libera da scopi diversi dalla pura prevenzione e protezione (altri obiettivi andrebbero solo a precludere la sua efficacia), consapevole dell’importanza di poter contare su una base di dati “volontari” (che vedremo meglio in seguito) per la gestione proattiva e dotata di tutti gli strumenti e le procedure necessari.

Inoltre l’articolo testimonia l’importanza di portare questa mentalità (anglosassone) nel nostro paese, per poter supportare il cambiamento culturale necessario ad una gestione proattiva dei rischi realmente capace di garantire un adeguato livello di protezione in contesti particolarmente complessi (come quello aeronautico ma non solo, anche in ambito industriale infatti abbiamo sempre più esempi di realtà complesse: centrali, piattaforme petrolifere, fabbriche con tecnologie particolarmente avanzate, ecc.; queste tecniche permettono anche di raggiungere alti livelli di protezione e prevenzione dei rischi in moltissimi ambiti, rispondendo così all’esigenza sempre più diffusa di una gestione proattiva del rischio).

La Just Culture prevede innanzitutto la creazione delle procedure e del sistema di gestione del rischio tramite lo sforzo congiunto e la collaborazione di tutti i livelli gerarchici dell’azienda, il tutto supportato dalle normative, volontarie e cogenti, disponibili.

Il secondo passo riguarda la creazione di un sistema di raccolta ed analisi di dati relativi alla sicurezza definiti “voluntary reports”, ovvero la comunicazione di eventi minori (guasti o anomalie minori riscontrati durante le operazioni o la manutenzione oppure i cosiddetti “near misses”, eventi che potevano diventare incidenti ma sono stati interrotti prima che portassero conseguenze gravi); entrambi vengono considerati “non mandatory” dalle normative.

Questi dati sono estremamente preziosi in realtà particolarmente complesse (intreccio di numerosi attori, procedure, sistemi, ecc.) perché, essendo praticamente impossibile prevedere tutte i modi possibili in cui un incidente può manifestarsi, questi report possono inquadrare degli scenari che in determinate condizioni potrebbero portare a gravi conseguenze e perciò mettono in luce delle criticità che sarebbero potute passare inosservate.

Capiamo quindi di avere a che fare con un vero tesoro di informazioni, che potrebbero aiutare risultare utili anche in altri campi, come ad esempio nella gestione della sicurezza sul lavoro e nella protezione degli asset (sostanzialmente l’affidabilità dei sistemi).

Tuttavia, affinché questo sistema di raccolta delle informazioni funzioni è necessario creare un rapporto di fiducia reciproca tra i vari livelli aziendali.

Infatti, nonostante le procedure di immissione dati utilizzino solo informazioni generiche (il sistema o le figure coinvolte nell’evento) necessarie a caratterizzare l’evento, in alcune situazioni è possibile risalire all’identità delle persone coinvolte. Pensiamo ad esempio al caso in cui solo due piloti siano assegnati al velivolo X e l’evento sia stato causato da un loro errore oppure il caso in cui un’azienda avente un solo tornitore e che riceva un rapporto riguardante un evento avvenuto su un tornio e che sia stato provocato dall’operatore ma interrotto prima di produrre conseguenze.

Risulta quindi estremamente importante che, salvo casi di negligenza grave, abuso o dolo (casi che verranno perseguiti nelle modalità previste), questi report vengano utilizzati

ESCLUSIVAMENTE per la gestione della sicurezza e MAI per identificare e perseguire le persone coinvolte salvo i casi appena citati.

Qui ci ricollegiamo con quanto detto prima: nel nostro paese è estremamente importante riuscire a portare una mentalità di questi tipo, capace di capire che la ricerca del capro espiatorio non è utile a nessuno, mentre una gestione come quella appena presentata non punta a lasciare liberi i colpevoli in nome della sicurezza, ma al contrario permette di giungere alle cause profonde e quindi di poter attribuire le vere responsabilità ad ognuno degli attori coinvolti, ed allo stesso tempo contribuire attivamente alla prevenzione degli incidenti.

La Just Culture potrebbe portare diversi vantaggi al sistema GRC di un'azienda, innanzitutto completando e riconfermando la sua cultura del rischio (funzione Risk) che fa della gestione proattiva del rischio una sua priorità.

In secondo luogo la raccolta e l'analisi dei voluntary report potrebbe non solo portare vantaggi alla gestione del rischio e delle normative, ma anche incentivare il personale a contribuire attivamente segnalando eventi particolari, potendo così aumentare la consapevolezza e la prontezza dell'intera organizzazione, potenzialmente in qualsiasi ambito.

Con questo si conclude il presente lavoro, e ci auguriamo che sia in grado di svolgere le funzioni, descritte all'inizio, che gli furono affidate in fase di progettazione.

Ci auguriamo inoltre che questo documento, oltre a fornire gli spunti necessari ad approfondire le varie tematiche e favorire un'implementazione di successo e proficua di questi sistemi, possa rappresentare il punto di contatto di un insieme di opere successive, ognuna focalizzate su uno dei temi qui trattati solo in maniera superficiale.

Tra le tematiche che ad oggi sembrano più interessanti e meno affrontate riteniamo che l'individuazione e l'analisi di tecniche gestionali (come quelle appena riportate) particolarmente affini ai sistemi GRC possa essere uno dei contributi più importanti e necessari alle aziende. Ciò potrebbe infatti scoprire e divulgare interessanti opportunità di completare ed arricchire questi sistemi, sfruttando al contempo sinergie ed affinità.

1. INTRODUCTION

Nowadays GRC integrated systems promise great benefits and consequently generate great interest in many fields, including industrial ones.

The present work wants to turn to the companies interested in GRC systems by supporting them in all the main phases and having three main objectives:

1. Show the potential of GRC systems as tools to improve business performance and solve some problems typical of “silo structures”.
2. Provide tools and guidelines for the selection and implementation phase so that the company can make these steps more in a more conscious way.
3. Provide cues to continue the improvement process and enable the company to make the most of the investment made on the new GRC system.

As we have said, this document turns to the staff of companies, for this reason the form and structure of this document have been designed to meet the needs of the readers, making an extensive use of lists in order to facilitate the reading and providing business cases or secondary data in order to support the discussion with practical examples.

The material consulted to create this documents is composed by articles, publication and documents written by consulting companies and interviews to CEOs of some companies that has successfully implemented an integrated GRC system and makes a continuous and profitable use of it.

First of all let's see briefly how the various points will be addressed during the course of this paper.

1.1 GRC systems and “silo structures”

The first step regards the presentation of GRC systems and their *modus operandi*, in order to correctly frame the topic of this project. Will be then provided some examples of how, inside companies, usually arise the needs to adopt an integrated systems such as GRCs; this should allow the reader to make a first comparison with the business reality of its company.

Finally, the second chapter will be devoted to presenting the “silo structure”, that represents the most widespread reality in medium-large sized enterprises, and presents its main issues to better frame the scenario in which GRC systems have been developed and how they intend to overcome those problems.

1.2 Tools and guidelines for the selection and implementation of a GRC system

The discussion will try to follow the path of a company once it takes consciousness of the need to adopt an integrated GRC system.

First of all, will be presented Forrester's framework for the creation of a business case aimed to calculate the ROI of the implementation and use of an integrated GRC system. This should help the CEO in creating a document to support the presentation, in front of the board of directors, of the proposal for the adoption of the new GRC system.

Afterwards, will be presented the study “*Big Picture for Governance, Risk, and Compliance Platforms*” made by of the Politecnico di Milano focused on showing and analyzing the GRC platform's evaluation and classification systems already existing and a new one created by its authors. This should provide to the staff of the company the information and tools needed to compare the various GRC vendors' offers and select the most suited ones.

At this point, chapter 4 will be devoted to present the requirements for successful implementation and a profitable use of the new system. This part was created by consulting the publications available online and the interviews to CEOs of some companies that have successfully installed an integrated GRC system and are making a continuous use of it, and are therefore able to provide important tips for the phases subsequent to the implementation.

Finally, chapter 5 contains guidelines for both the implementation phase and the creation of the optimal conditions for a proper and profitable use of the new system during normal operating conditions, thus enabling the company to reach the benefits presented in this document.

1.3 Tips for future development

The last part concerns the phase subsequent to the successful implementation of the new integrated GRC system. It aims to help and support the company in continuing its improvement process through the identification of policies, methodologies or tools capable of supporting and completing the new system. For this reason, two management techniques particularly aligned with the philosophy and modus operandi of the GRC systems has been selected and provided. They represent a great opportunity to enrich and complete the new system in an easy and cost saving way, exploiting some advantageous synergies.

The two techniques in question are: the BYOD policy (relating to the management and use of personal devices for business purposes) and the so-called "Just Culture" (dealing with risk management culture and procedures).

2. GRC SYSTEMS

2.1 GRC Systems

The acronym GRC stand for: Governance, Risk, and Compliance Management but, in order to give a definition of what is considered to be a GRC System, we can refer to the article “GRC – The Pathway to Principled Performance” available on OCEG.org.:

“...The acronym GRC was invented as a shorthand reference to the critical capabilities that must work together to achieve Principled Performance¹ — the capabilities that integrate the governance, management and assurance of performance, risk, and compliance activities.” and later “It is important to remember that organizations have been governed, and risk and compliance have been managed, for a long time — in this way, GRC is nothing new. However, many have not approached these activities in a mature way, nor have these efforts supported each other to enhance the reliability of achieving organizational objectives. In a forward-thinking organization, GRC is viewed as a well-coordinated and integrated collection of all of the capabilities necessary to support Principled Performance at every level. GRC doesn’t burden the business, it supports and improves it. — in this way, GRC is totally revolutionary.”.

This gives us all the information needed to introduce GRC Systems: they can be considered as tools to support the organization in reaching its objectives and achieving a more efficient and effective use of its own resources.

As we mentioned before GRC are composed of three parts: Governance (knowledge management), Risk (risk management), and Compliance (regulatory compliance); also if we consider the GRC platform available on the market we have the possibility to purchase the complete system (what we call “integrated GRC system”) or only one or two of its components.

In this document we consider just the case of integrated GRC systems as they represent the only way to make the most of their potential and achieve the benefits.

First of all could be useful to investigate what usually push companies to consider the purchase of an integrated GRC system.

2.1.1 GRC drivers and how the need of an integrated GRC arises

OCEG call these factors “GRC Drivers” and we can report some examples:

- An increasing management complexity due to the dynamism of the environment in which the company operates
- Stakeholders demand high performance along with high levels of transparency.
- Regulations and enforcement are ever-changing and unpredictable.
- Exponential growth of third-party relationships and risk is a management challenge.
- The costs of addressing risks and requirements are spinning out of control.
- The harsh (and scary) impact when threats and opportunities are not identified.

¹ OCEG considers Principled Performance as an approach to business to achieve objective while coping to uncertainty. The three pillars of Principled Performance are: Principled Pathway (break down silos and leverage common capabilities in every key system that keep an organization on track; this is very close to the way GRC systems acts), Principled People (Leadership, the workforce and extended enterprise must be populated by principled people with strong character and a commitment to competence who consistently direct their energies toward a principled purpose), and Principled Purpose (A principled purpose is perhaps the most basic starting point for principled performance. Defining your highest purpose via mission, vision and values guide everything that the organization does.).

In Italy the first sectors that have adopted an integrated GRC system are Finance (whose first concern is security and risk management) and Telecommunication (whose first concern is compliance, as a consequence of the strict rules to which it is subject); however we can see some examples of companies operating in the industrial sector that are beginning to look at GRC as a way to achieve better control and flexibility.

CryptoNet, an Italian company specialized in IT security and business software, has published on its site an article regarding GRC in which identifies the “compliance function” as the process from which usually arises, inside a company, the need of structured and more efficient procedures. In fact, most of the times, daily compliance processes are carried on in an irrational way, conducting interviews and creating reports; CryptoNet mentions annual complies to d.lgs. 196/03 and 231/01 or l. 262/05 as examples of processes that in most of medium or large enterprises born and dies periodically resulting in an inefficient use of resources. In other words they consider only the “immediate problem” they are facing at the moment without looking for the identification of the elements common to all the activities, in order to be able to automatize these processes.

This would allow us to get significant benefits like reducing direct costs or start working in an incremental way in order to enhance company awareness and create a process of continuous improvement.

However compliance is not the only process from which the need of an integrated GRC system may arise: nowadays also the need of an ever greater ICT security, becoming critical due to the choice of using web as a business tool in a more extended way, push in the same direction asking for more aware and effective procedures.

Those are two examples of “symptoms” of the need of a more structured and coordinated system and so the company should not concentrate only on the specific problems regarding for example only compliance or ICT security but should consider this as an opportunity to make a significant change to the way it manages its operations and to solve at the same time a lot of problems, that share some common causes even if the company may not be aware of it.

2.1.2 The benefits of an integrated GRC system

As we can imagine this kind of decision could be frightening because it involves the entire company or because it requires a lot of resources and a long time for its completion; however also the benefits arising from the adoption of an integrated GRC system are equally attractive:

- Enhancing company awareness about its resources and potentiality through a centralized management of information.
- Enhancing company effectiveness through the creation and use of structured procedures to perform all business functions.
- Enhancing company efficiency taking advantage of the information coming from the centralized information management system.
- Enhance company effectiveness facilitating top manager’s decision making process providing a constant flow of complete and updated info in order to take more aware and quick decisions.
- Increase company stability and resilience through a better risk management that attempts to identify and eliminate the root causes common to multiple different problems in order to act in a more effective and efficient way.

Later on we will see how to calculate the ROI of an integrated GRC platform by presenting a framework created by Forrester (one of the most influential research and advisory firms in the world) to help CEOs in preparing a business case to better present the proposal to adopt a GRC to the board of directors.

2.1.3 Implementation phase

As we can imagine the best scenario would be a green field project in which we can create ex-novo an integrated GRC system. However most of the times reality is far different and we could face situations in which there are several pre-existing investments made in different functions (e.g.: IT department) that need to be protected and at the same time “siloes” structure and mentality difficult to eliminate.

In this case there are a lot of different solutions that may be chosen, but we can divide them in two different categories:

- **“less invasive”** procedures: focuses on the creation of a centralized information management system integrating all the different solutions adopted by individual departments. This choice represent a trade off between the requirement of the new integrated GRC system and the old company structure but if we choose this path we need to be conscious that we would carry many of the “old problems” into the new system and we could also create some new ones;
- **“more invasive”** procedure: redesign, one department at a time, every corporate function in a mutually-integrated way, in order to leave “old problems” behind.

The second category is for sure the most interesting and difficult of the two and so will be the one on which this work will focus.

Most of medium and large enterprises have “silo structures” in which every function works autonomously (with its own hierarchical structure and objectives) and in which poor communication and coordination becomes the main source of problems. For this reason we will devote one of the chapter of this document to better understand the “silo structure” and its problems in order to clarify the importance of integrated GRC systems and how they solve this kind of situation.

In the rest of this chapter we will look more closely to the three parts of GRC (Governance, Risk, and Compliance) and then provide two important documents: Forrester framework (that we mentioned before) and *“Big Picture for Governance, Risk and Compliance Platforms”* created by Politecnico di Milano.

2.2 Components of an integrated GRC system

2.2.1 Governance

Governance can be considered as the backbone of an integrated GRC system and concerns the management of corporate knowledge. It requires the creation of a central information management systems that collects, analyzes and makes available data coming from all the departments of the company.

The system requires the integration of three parts:

1. **Hardware:** usually it requires just a web server, an application server and a database.
2. **Software:** the company has many options and can choose the most suitable software for its needs. Usually the parameters that affect this choice are the extent to which the company intends to use the system and the number of workers authorized to interact with it.
3. **Training:** as we will see in the chapter 5, training is one of the most critical elements. In fact if workers won't feel comfortable in using the new information system they may decide to use other communication systems making the investment vain.

As we said the information system collects, analyze and elaborate the data in order to support the top manager in the decision-making process. In order to do so the data must meet certain requirements:

1. **Be Complete:** all the information needed to characterize a product, a process, a customer or any other object of interest for the company must be grouped together. For example if we are dealing with Product X we need to collect data from all the departments in order to create a complete set of information. In this case we would need:
 - Technical data coming from production department.
 - Sales data coming from marketing department.
 - Data regarding the supply chain coming from the supply department.
 - Data regarding the voluntary and binding regulations to which the product must comply.
 - Data relating to the handling and storage of resources need for the production.
 - Safety data regarding production processes.
 - Data regarding all kind of operational risks (e.g. SCRM).
 - Etc..
2. **Be updated and free of redundancy:** same data regarding the same object (created in different moments or by different workers) cannot exist at the same time inside the information management system. Otherwise the efforts to determine which copy is the right one would result in a waste of resources and may lead to take decision based on incorrect or outdated data.
3. **Be uniform:** inside a "silo structure" is not uncommon that different departments use the same word with two different meanings, but since the interaction between them is very poor this is not a big issue. Now we are "forcing" all the departments to work together in feeding the new information management system and so it's mandatory to create and use a common language in the entire company. This enables the information management system to analyze and aggregate the data coming from all the different departments.

To conclude we can list some of the benefits brought by the GRC knowledge management:

- Improve company awareness about its process and resources (so we are able to avoid useless duplications and to identify and exploit synergies).
- Improve company awareness about both internal and external risks that may impact its performances.
- Improve company awareness about market requirements and competitors in order to take strategic decisions to gain competitive advantage.
- Involving all the departments in a common effort (feeding the centralized information management system) creates greater cohesion and spirit of collaboration, resulting in better ability to identify and report problems and coordinate the efforts to align with the goals set by top management.
- Allow top manager to take quicker and more conscious strategic decisions by providing a constant stream of updated data.
- Improve company capability of collect and analyze data to learn from past events and capitalize corporate knowledge (e.g.: creating new procedures or updating and improving existing ones).

2.2.2 Risk

Nowadays most of the companies manage risk following the principles of ERM:

1. **Identification** of events and circumstances that may have an impact on corporate objectives.
2. **Quantification** of any single risk by considering its occurrence probability and severity of consequences.
3. **Determination** of the necessary corrective actions and barriers.
4. **Monitoring** progresses and repeating cyclically the identification phase to detect new risks.

One of the scopes of *"Big Pictures for Governance, Risk and Compliance Platforms"* was to investigate the relationship between ERM and risk management system of integrated GRC systems considering the opinion of experts. Authors concluded that exist two schools of thought: the first one argues that ERM and its components represent the Risk part of GRC systems, the second one (supported by the authors of the *Big Picture*) argues that the two approaches share some processes and technologies but largely differ for the basic concept.

They claim that ERM analyzes risks by taking a snapshot of the system at a precise moment and proposing the corrective actions to be implemented; GRC systems instead highlight the most critical processes, allowing both aggregate and detailed views to improve corporate resource awareness and to make full use of their the potential.

The fact that available information are kept updated allow the company to conduct a constant risk control, detecting quickly any deviations from normal operating parameters (for example monitoring KPIs), identifying possible causes (internal/external to the company, direct/root) and increasing the company's responsiveness and resilience.

It is clear then that, as we said before, both the Risk part and the Compliance part depend entirely on the Governance part, in particular on its centralized information management system.

Furthermore the philosophy on which GRC are based want to turn risk and compliance management into a cross sectional component of all corporate processes, in order to homogenize them into daily operations and help to create a way of thinking and acting more structured and conscious (in chapter 5 we will see more in detail how is possible to turn risk and compliance management into all other processes in a sustainable way).

Consequently, the determining factor for the success or failure of such a system becomes the "human factor", and more particularly the mentality of users that will require a change from before. Corporate culture management is now one of the most critical elements for a company that needs to change and although the difficulties and long times needed for such a process could discourage similar initiatives, almost all modern management techniques require a change of this kind. We will resume this topic in the final chapter when talking about "Just Culture", a risk management technique used in aviation which is perfectly aligned with the philosophy of GRC systems and thus represents a good way to continue the improvement process of the company begun with the adoption of an integrated GRC system.

As before, we can conclude this brief focus about risk management in integrated GRC system listing some examples of possible benefits:

- Improve company visibility of all its processes in order to identify criticalities and implement adequate barriers.
- The great amount and variety of data coming from the centralized information management system improves company capability of managing external and complex risks (e.g.: SCRM, supplier selection risks, etc.).
- A more advanced and effective risk management system allows the company to have a more robust and detailed risk profile with the following advantages:
 - Improved company stability and the ability to have a competitive advantage.
 - Greater attractiveness for contracts, acquisitions or joint ventures.
 - Credits and insurance under more favorable conditions.

2.2.3 Compliance

Speaking of regulations, we can first distinguish between binding norms (mandatory in order to operate in a particular sector) and voluntary standards, the latter being increasingly important nowadays. In fact, rival companies compete one with each other on many fronts, including the image perceived by the customer. Watching commercials or visiting a company's web site we may well notice the great attention paid to the ethical criteria adopted, the sustainability of the processes and the quality of the company's products.

All of these components strengthen the company's public image, gaining customer confidence and loyalty in order to differentiate and take advantage over competitors. Voluntary or binding norms (e.g.: ISO: 9001 for quality management, ISO: 14000 for environmental management, ISO: 22000 for food safety, etc.) to which the company complies attest the adaptation to the standards provided and give in return a certification that can be exhibited.

The issue of compliance management is not about the investment made for the tools (usually simple spreadsheets are used, e.g.: Excel) but regards the amount of resources needed to monitor the updates of the various regulations, especially as the number of standards (usually voluntary) chosen by the company grows too much.

Choosing to invest in software for regulatory compliance management allows the company to transfer the burden of keeping the set of rules (voluntary and binding) updated to the supplier in order to free and to reallocate internal resources. If we consider this type of

software integrated into a system such as GRC, we can easily bring compliance into any other business process, making it more homogeneous and lightweight to manage, enabling the company to adhere to new standards.

We can now list some of the advantages of using a GRC for compliance management:

- Allow the company to free and reallocate internal resources.
- Allow the company to adhere to a greater number of standards in order to take over competitors or being able to enter new markets governed by different regulations.
- Reduce the risk and impact of legal costs or penalties for non-compliance.
- Reduce the risk of image loss resulting from violations.

2.3 Calculating the ROI of an integrated GRC system

When a company intends to purchase a GRC system, it will be necessary to submit a request to the board of directors. The authors of *"Big Picture for Governance, Risk and Compliance Platforms"* identified the three business figures that could participate in the selection of a GRC system: CRO, CIO and CFO. One or more of these figures will have the task of persuading top management of the benefits of using such platforms to justify the necessary effort in terms of time and resources.

Forrester suggests addressing this topic by following three steps: cost estimation, benefits estimation, and risk analysis.

2.3.1 Cost estimation

As we said, the first step concerns the identification and estimation of the main cost items. The investment required by this type of product varies between 200 and 700 k€ and GRC vendors offer a "package" that usually includes: software, hardware, and implementation services.

The final cost usually depends on several parameters: company size, software required features, number of regulations to be included in the system, number of users, etc.. With "number of users" we mean the number and type of profiles to be created in order to interface with the information system. As we mentioned, the new centralized information management system will be constantly fed with data coming from all business functions and in the mean time it will provide some information to specific roles inside the company. For those reasons we need to profile all the personnel to assign the right and necessary credentials and access rights (data entry, data visualization, data entry & visualization) to each single worker that will become a user. This ensures an adequate level of security (sensitive information protection) and the possibility for users to participate in a conscious and active way.

Usually the investment required for the hardware part of the system has a minimal impact on the overall cost; GRC systems in facts require just a web server, an application server, and a database (the size of these tools will depend on the size of the business and on the use that the customer intends to do).

Instead, the support of the GRC vendor may take several form: in some cases it will be necessary to have at least one full-time resource for every 50-75 active users for IT support within the company; in other cases, it will be sufficient to require strategic and organizational advice (not essential for the implementation of an integrated GRC system, so it may be neglect during cost estimation).

Also in case of software-as-service or hosting solutions we would have the same types of costs we just identified and will be embedded into the subscription fee.

2.3.2 Benefits estimation

Forrester identifies three main categories of (medium to long term) benefits that a GRC platform can bring to our company: **Efficiency**, **Risk Reduction**, and **Strategic Performance**.

Category	Examples	Example calculations
Efficiency	<ul style="list-style-type: none"> • Policy and control management (faster development, review, update, approval, distribution, access, and attestation) • Risk management (faster risk identification, analysis, evaluation, and monitoring) • Audit management (improved scoping, scheduling, data collection, and reporting) • Compliance management (easier association of controls, control assessments, assessment data aggregation, and reporting) • Action management (faster event identification, notification, escalation, remediation, review, and approval) 	<ul style="list-style-type: none"> • Hours saved per function multiplied by the average rate for fully burdened risk, compliance, or audit professionals • Payroll savings from delay or avoidance of staff increases • Reduction in costs of external audits and assessments
Risk reduction	<ul style="list-style-type: none"> • Improved compliance (fewer audit findings, regulatory enforcement actions, and lawsuits) • Improved risk treatment (prioritized and faster remediation) • Improved risk posture (lower cost of capital and insurance premiums) 	<ul style="list-style-type: none"> • Reduction in incident response costs • Reduction in the number and size of fines and penalties • Increase in risk exposure mitigated per dollar/hour spent • Reduction in cost of capital • Reduction in insurance premiums
Strategic performance	<ul style="list-style-type: none"> • Greater oversight (fewer unexpected loss events, accurate view of risk and compliance posture) • More informed decisions (related to development, procurement, and investments) • Better performance (more successful product launches, market expansions, branch openings, technology implementations, or partner engagements) 	<ul style="list-style-type: none"> • Reduction in costs required for unexpected, short-term injections of capital, staff, or other resources • Greater amount of relevant data to support decision-making • Increase in financial or on-time performance (business units, partners, projects, etc.)

56677

Source: Forrester Research, Inc.

Figure 4: Types of benefits of an integrated GRC system (Source: Forrester Research, Inc.)

Forrester provides tangible examples of benefits but, while the increase in efficiency or risk reduction can be quantified by considering the amount of saved hours or the reduction of costs or sanctions, the benefits of "Strategic Performance" are more difficult to be express in a practical way. This kind of benefits are the same that we have identified in previous chapters: greater awareness of the environment in which the company operates and more aware choices (greater knowledge of the market and competitors = more successful products, reduction of negative consequences, more successful development choices, identification of new opportunities, etc.).

Forrester tries to clarify better this topic by considering two distinct kinds of flexibility:

1. **Extensibility of investment:** investment on a GRC platform, albeit high, allows substantial savings when deciding to add new features; (This is the case for example of Business Continuity platforms: 40 k€ to add a module to the GRC against 400 k€ for the ex-novo solution)

2. **Agility in Business Support:** Forrester intends to emphasize the fact that a GRC platform facilitates the company's entry into new markets or integration with new partners, businesses, suppliers, or workforce. More in-depth the use of a GRC reduces the costs associated with requirements definition, due diligence activities, and compliance training.

The following table tries to summarize what we just said:

Category	Examples	Example calculations
GRC extension flexibility	<ul style="list-style-type: none"> • Using the platform for multiple GRC domains (i.e., business continuity, IT, environmental, financial, etc.) • Ability to react quickly to new and changing regulations 	<ul style="list-style-type: none"> • Estimated cost savings from platform consolidation (i.e., spending \$30,000 to \$40,000 on the business continuity module of a GRC platform versus \$200,000 to \$400,000 for a standalone business continuity management platform) • Cost to configure GRC platform for new regulatory content versus cost of a new compliance management product
Business agility flexibility	<p>Smoother integration of business partners, acquired entities, new employees, etc.</p>	<ul style="list-style-type: none"> • Number of hours (or days) of reduced compliance training and ramp-up time multiplied by productive output of new employee, partner, or acquired entity • Reduction in time and costs of compliance/risk due diligence before strategic decisions • Reduction in opportunities missed because of a lack of compliance/risk insight

56677

Source: Forrester Research, Inc.

Figure 5: Components of "Strategic Performance" (Source: Forrester Research, Inc.)

2.3.3 Risk analysis

This third and last part deals with the identification of risks connected to this kind of projects (for some of them we will try to propose some solution in chapter 5):

- Costs and delays resulting from unforeseen events or necessary skills not identified during the design phase.
- Resistance to adoption by users: greater involvement required during the implementation phase.
- Problems of integration with pre-existing IT platforms.
- What Forrester calls "**vendor viability**": SVM professionals define vendor viability as the combination of the vendor's inherent riskiness and their firm's tolerance for supplier-related risk. In other words we are considering the case of companies that consider the relationship with their supplier vital for the success of their business or projects and therefore expose themselves to a particular set of risks. The company has two types of control over this kind of risks: when selecting the most appropriate supplier the company has a "direct" control because, if it manages to collect all the needed information it can create a precise profile of every candidate and focus on the most concerning elements. Then after the beginning of the relationship with the selected supplier the control of the company over those risks becomes "indirect", meaning that will be difficult to fully monitor the supplier and take corrective actions.

GRCs are a perfect example of this kind of situations: GRC vendor does not only provide the initial “package” but is also responsible for keeping it always performing and updated according to the needs of its customer. Forrester therefore considers "vendor viability" as an indicator of the reliability of the GRC vendor and consisting of two parts:

- **"vendor inherent riskiness"** (as if it was the "intrinsic risk" of the vendor, can be seen as the risk profile of the supplier considering the risks to which it is exposed or decides to expose and the protections it has implemented).
- **"firm's tolerance for supplier-related risk"** (how much our company is exposed to GRC vendor's risks, in other words it measures how much the enterprise is protected or what would be the consequences in case the vendor GRC should suffer a disruption).

It is obvious how much this type of risk depends on the combination "company-vendor", and therefore it requires a number of studies during the design phase.

2.3.4 Summing up

Let's summarize what we just said by creating a scheme of the steps required to calculate the ROI of an integrated GRC system:

1. **Costs estimation:**

- a. Software;
- b. Hardware;
- c. Profiling;
- d. Support;
- e. Advice;
- f. Various.

2. **Benefits estimation:**

- a. Increased efficiency;
- b. Risks reduction;
- c. Strategic performance;
 - i. GRC extension flexibility;
 - ii. Business agility flexibility.

3. **Risk Analysis:**

- a. Costs and delays due to unforeseen events;
- b. Resistance to adoption by users;
- c. Integration problems with pre-existing IT platforms;
- d. "Vendor Viability"

2.4 *Big Picture for Governance, Risk, and Compliance Platforms*

In this chapter we will briefly present the work "*Big Picture for Governance, Risk and Compliance Platforms*", developed by Andrea Brusa Perona, Ing. Guido Jacopo Luca Micheli and Prof. Enrico Cagno.

The project has been divided into three parts:

1. The study of GRC systems, underlining the benefits of using an integrated system.
2. The study of existing evaluation and classification systems and the development of a new one.
3. The application of the new rating and classification system, considering the GRC platforms directly available on national territory.

2.4.1 GRC study

The first part uses data from publications and interviews to CEOs of some major Italian companies to present the main features of GRC systems (some already mentioned in the previous chapters) and comparing the two options of adopting a GRC platform: by purchasing it ("buy" option) or by creating it inside our company ("make" option). The authors concludes that "buy" option is the only one that can bring real benefits to the company, because of several considerations (some of them already shown in the previous chapters):

- Relying on a supplier allow the company to transfer the burden of keeping compliance database always updated.
- Internal creation of a GRC platform would require higher resources and longer time than purchasing and implementing a finished product.
- Relying on a finished, tested and certificated product will result in greater guarantees of successfully implement a system that works as planned and has good reliability.
- Etc..

Finally the authors compare pro and cons of choosing an integrated GRC system or just a part of it (e.g.: just Governance part), concluding that an integrated GRC system is the only one that can solve the problems of a "silo structure" (we will address this topic deeper in chapter 3).

2.4.2 Existing GRC evaluation and classification systems

The second section begins with the analysis of the two existing evaluation systems: Gartner's "*Magic Quadrant for Enterprise Governance, Risk and Compliance Platform*" and Forrester's "*Forrester Wave: Governance, Risk, and Compliance Platforms*". Both classify GRC systems using a comparative matrix resulting in a relative ranking between the platforms being considered and attaching a detailed descriptions of the various software in order to highlight strengths, weaknesses and recommended application areas.

The authors of *Big Picture* claims that although these tools allow for an intuitive and quick-to-use classification, identify the most financially strong GRC vendors and track the evolution of platforms performance (comparing several editions of the publications), they have limitations of completeness.

First of all, they consider only the largest GRC vendors (in terms of customer base or turnover) ignoring a large part of the existing market and conducting just a superficial

analysis of some of the major aspects of GRCs such as the content offered. These limitations emerged also from the interviews with some Risk Managers who complained of the inadequacy of these tools in supporting the choice of the most suited GRC system for their needs, forcing them to contact consultants and industry experts.

From these observations emerged the need to develop a new classification system, which completes the two previously mentioned tools, with the specific aim of helping companies identify the GRC system best suited to their situation and at the same time allow GRC vendors to show the features of their products.

For this reason, the authors of *Big Picture* chose to include all the available platforms on Italian territory, without limitation on the size of the vendors.

The proposed instrument consists of two parts: "Evaluation" and "Classification".

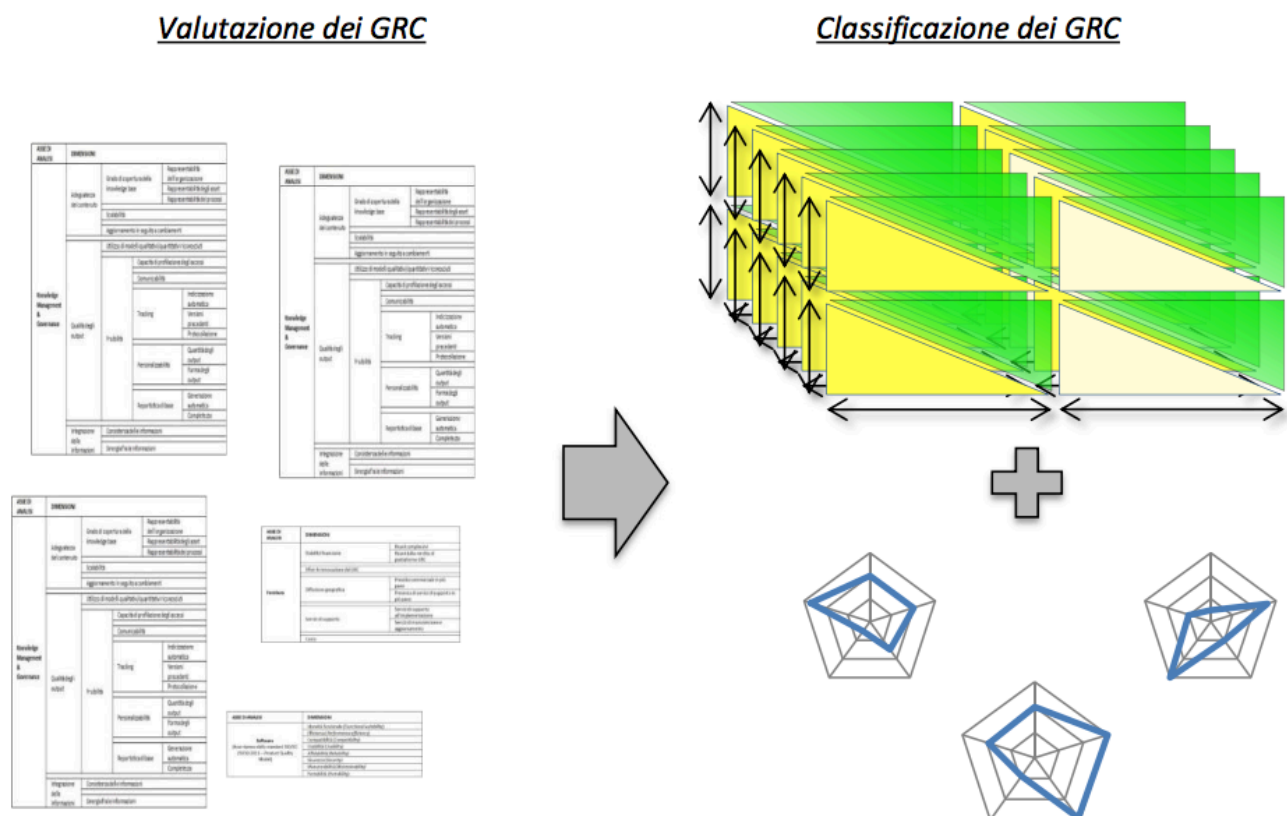


Figure 6: Showing the structure and tools of the new evaluation and classification system developed by the authors of *Big Picture* (Source: *Big Picture for Governance, Risk and Compliance Platforms*)

2.4.3 The new evaluation and classification system

During the “Evaluation” phase three criteria of choice are considered: **Content**, **Software** and **Supply** (those three aspects can be linked to the three corporate figures involved in the decision to purchase a GRC system: CRO, CIO and CFO).

The “Content” criterion is considered for each of the three functions (Governance, Risk and Compliance) and is composed by 3 indicators: Content Adequacy, Output Quality, and Feature Integration.

The “Software” criterion follows the guidelines of ISO/IEC 25010:2011 and is characterized by the following indicators: Functional Suitability, Efficiency, Compatibility, Usability, Reliability, Security, Maintenance and Portability.

The “Supply” criterion considers the probability of success and satisfaction with the investment in a specific GRC system, considering five macro-dimensions: Financial Stability of

the Provider Company, GRC Innovation Effort, Geographic Spread, Quality of Services Support offered and Purchase Cost.

The "Classification" phase starts creating the criteria to aggregate all the indicators considered during the "Evaluation" phase in order to get a graphical representation of the results using matrices and radar graphs.

Platform evaluation is based on a benchmark analysis of the same, considering two scenarios, based on the relative importance of the content provided by the GRC and not on their possible uses, trying to overcome one of the limitation of the other two classification tools. The two scenarios are named "Balanced Contents" in which the three axes (Governance, Risk and Compliance) weight 1/3, 1/3, 1/3, and "Governance Based", in which the Governance axis has a weight of 50% while the other two equally divide the remaining 50%.

By doing this the authors try to help the companies interested in purchasing an integrated GRC platform that may want to use the new system in different ways.

The classification system creates 5 matrices having on the "X axis" the evaluation of the "Software" Criterion and the "Y axis" one of the 5 indicators listed above. Each axis is then divided into two ("high" and "low") parts, resulting in a matrix with four quadrants that are divided again into two in order to create binary bands and to reduce the error resulting from a too punctual rating.

The classification is conducted by interviewing the most satisfied customer, because is the most suitable subject to highlight both the potentialities and the limitations of the product.

The GRC platforms are compared to each other and placed in relative position inside the matrices, making the tool solid and able to evaluate any combination of GRC systems (starting from just two platforms up to, ideally, all those available on the market) to help the company in selecting the most suitable product for its needs in the most simple and immediate way.

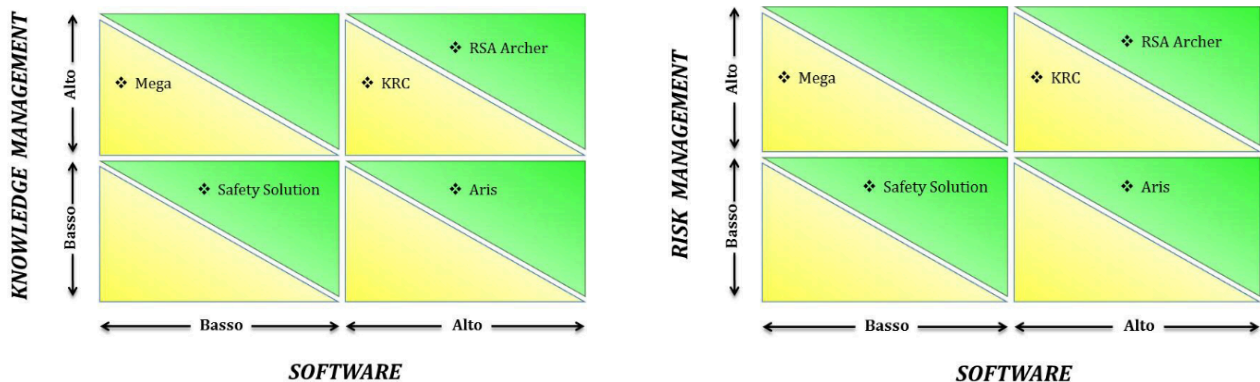


Figure 7: Examples of the matrixes used during the "Classification" phase
 (Source: Big Picture for Governance, Risk and Compliance Platforms)

The last step is the creation of a tab that summarizes all the relevant information (characteristics of the supplier; product features, strengths, weaknesses and improvements; the user interviewed for the evaluation) and a radar graph that summarizes the results of the classification phase.

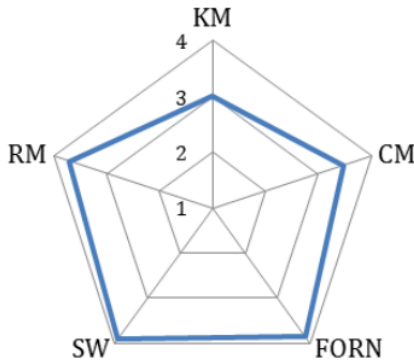
<p>SW Vendor</p> <p>Software AG, storica azienda tedesca produttrice di un'ampia gamma di software, è annoverata tra le prime venticinque a livello globale ed opera in oltre 70 paesi direttamente coperti tramite una rete di partner e servizi localizzati. Ricopre il ruolo di player chiave anche nel mercato italiano per quanto riguarda le soluzioni GRC.</p> <p>Sito aziendale: http://www.softwareag.com/it/</p>	
<p>Prodotto</p> <p>La piattaforma Aris Risk & Compliance Management è cross industry e personalizzabile per ogni cliente sulla base delle sue specifiche necessità.</p>	
<p>Punti di Forza</p> <ul style="list-style-type: none"> → Sistema fortemente integrato con l'ambiente di modellazione dei processi e integrabile con gli altri sistemi interni aziendali; → Schermate e processi di lavoro (“<i>workflow</i>”) chiari e ben definiti; → Solida metodologia sottostante. 	
<p>Punti di debolezza e/o miglioramento</p> <ul style="list-style-type: none"> → Sono richieste diverse personalizzazioni per migliorare il livello di efficienza del sistema. 	
<p>Utente valutatore</p> <p>Banco di Desio e della Brianza: è una delle più importanti realtà bancarie sul territorio nazionale, che conta più di 270 filiali distribuite tra Nord e Centro Italia.</p> <p>Sito aziendale: https://www.bancodesio.it</p>	

Figure 8: Example of Summarizing Tabs and Radar Graphs
 (Source: *Big Picture for Governance, Risk and Compliance Platforms*)

3. SILO STRUCTURES

The aim of this chapter is to present the so called "silo structure" and highlight some of its typical issues to better contextualize the scenario in which integrated GRC systems have been born and what problems they intend to solve.

3.1 What is a silo structure and why is used

With the advent of globalization, the boundaries within a company operate became wider (in some cases they disappear: companies operating all over the world) and this has brought new opportunities and new challenges.

The environment in which companies are currently operating is characterized by an intrinsic complexity and is in a constant change; this implies that an enterprise is exposed to the action of multiple forms of uncertainties, which have direct or indirect effects on its performance and its competitiveness. We can try to better clarify what we are talking about by presenting some examples of sources of uncertainties and their effects on businesses:

- Market growth: the market in which companies are operating may be more or less extended (up to reach the global market), but remains characterized by continuous and rapid changes due to several factors:
 - Legislative and regulatory changes that can open new markets (liberalization), preclude some existing ones (embargoes) or somehow limit certain types of products (more stringent controls and requirements).
 - Competitors' actions that may increase their market share by exploiting new opportunities.
 - Poor decisions or suffered disruption that may provide others an opportunity to become stronger and expand.
 - Demand fluctuations due to more or less predictable mechanisms (trend, seasonality, fashion effect, competitor behavior, etc.).
- Technological innovation: nowadays it is almost essential to remain competitive while maintaining efficiency and effectiveness. Choosing the adequate level of technological innovation is usually a trade-off between the performance that the company wants to guarantee (defined by top management's business strategy: usually the market share that the firm decides to control or the balance of power with other competitors) and how much is willing to invest in "chasing" technological progress.
- Supplier behavior: when a company becomes part of a production chain, it is exposed to a number of risks related to the fact that some of its performance depends on the behavior of external parties when carrying out their operations. We can list some of these risks:
 - Logistical risks: incorrect quantities and/or timelines not respected.
 - Loss of expertise: when a company outsources a part of its operations, it loses skills that are hard to recover in the future.
 - Loss of control: this kind of risk is closely related to the previous one and occurs if the company has to integrate parts, components or products coming from suppliers. The first risk we may think about is directly related to the "quality control": the company establish an internal control mechanism to keep under control the defectiveness of the input parts and avoiding extra costs for reworks or overproduction. But we have to be careful because this kind of situation can hide much greater risks that may lead to far more serious consequences. We can take as an example what happened to **Mattel in 2007**. Mattel, the famous toys manufacturer, had to withdraw thousands of non-compliant products from

the market due to some components manufactured in China that contained an unacceptable level of lead (Pb). So the problem is linked to a lack of control over the supplier and the inappropriate materials used. All this has caused to Mattel, not only a financial cost related to the withdrawing of all the non-compliant products, but also a major image damage, especially large because we are talking about a very sensitive sector: children's health and safety.

- Human resources management: the evolution of technologies and management techniques used, the degree of innovation and complexity of products, the size of production volumes and their change (expansion / resizing needs) may lead, in some cases, to large difficulties in managing the personnel, in particular for identifying the required skills and sizing the number of operators.
- Financial management: has become a very serious problem for a large number of companies, especially as a result of the economic crisis, with great difficulty in obtaining loans to carry out normal operations (e.g.: pay the suppliers), to fund R&S projects, to exploit opportunities (ancillary production, expansion, entry into new markets or niche markets, etc.).
- Relationships with customers that can take different forms:
 - Market surveys to identify customer requests.
 - Effective advertising campaigns (for example, in the automotive sector, where one of the most important elements that affect car sales is the media coverage of the model).
 - Pre/after sales support to the customer (selection of the most suitable product, installation, advice, training, maintenance/replacement/disposal, etc.).

The need to manage a so large and varied set of operational risks has pushed many companies to try to protect the so-called "core functions" (those considered by the company as the main activities that create value in the product, this can be applied to both manufacturing companies and service providers) using other business functions as "buffers" against the various forms of uncertainty. The following image tries to clarify what we just said: the central rectangle represents the "core functions", the ellipses represent the "buffer functions" and some examples of uncertainties are reported in bold; those uncertainties are "filtered" to allow the core functions to operate in a determined environment.

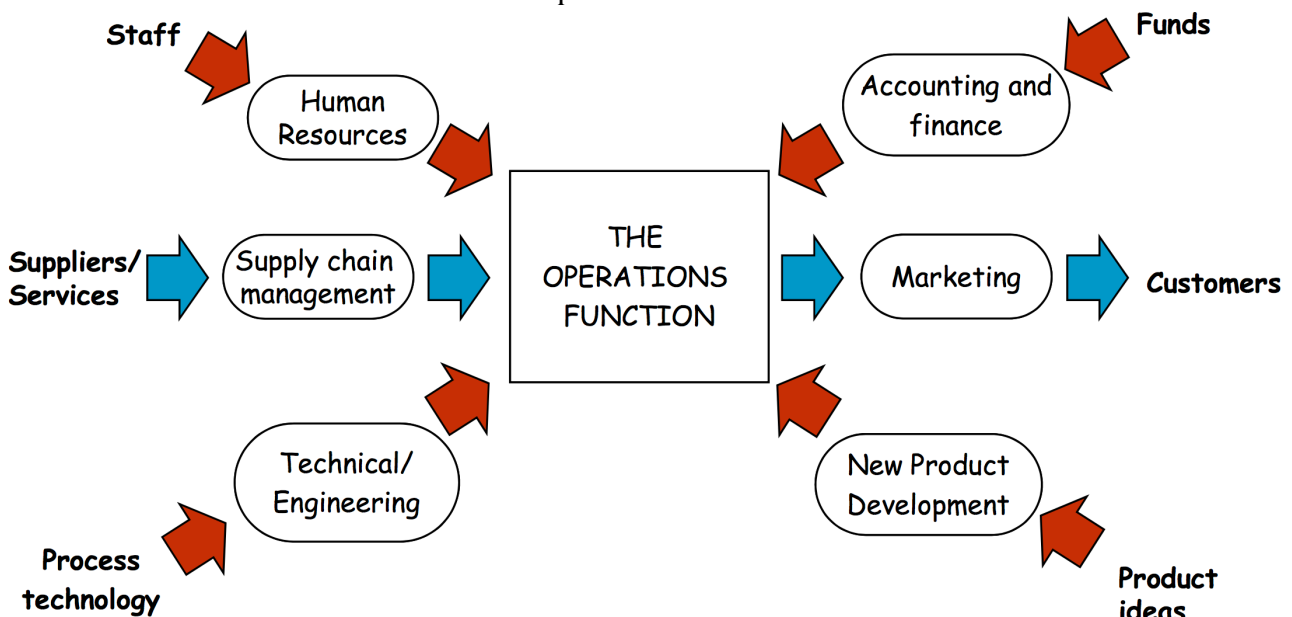


Figure 9: Schematic representation of a "silos structure" (Source: Industrial Risk Management Course)

This creates a structure that is now typical of many large companies where business functions (e.g.: marketing, production, product design, etc.) are fragmented into distinct sectors that operate as autonomous entities, each having their own objectives (local objectives) and hierarchical structures.

The aim of using a silo structure is to streamline company management while simultaneously addressing the effects of market-to-business interaction more easily.

To make an example we can resume the structure shown in the figure and consider the case of a company interested in "protecting" the production department. As a result, the other departments (e.g.: marketing, human resources, logistics, etc.) become autonomous units with the task of managing their own type of uncertainty coming from the environment in which the company operates. Since then the marketing department will handle the demand fluctuation, the logistics department will guarantee the continuity and quality of the input materials, the human resources department will provide staff with the necessary skills, and so on. This allows the core functions to operate in an environment without any uncertainty (for example the demand forecast arrives at the production sector as quantities that it has to provide) so that they can perform their operations in the most efficient way possible, reducing costs and thereby increasing the profit margin.

All this has undoubtedly allowed companies to gain great benefits (especially in reducing overall management complexity) but what we actually get is that problems arising from the various forms of uncertainty are shifted from core functions to other departments rather than being tackled and resolved.

3.2 The issues of a silo structure

Choosing to make the various business functions autonomous to reduce management complexity will result, most of the times, in a loss of coordination and communication between all the different departments, leading to a loss of efficiency and the formation of some serious, and usually latent, problems which, as will be shown below, are the cause of many complications that may arise in the company.

We will now present some of the main problems associated with poor communication between the different departments:

- **Communications delays:** usually there are official meetings and events where the representatives of various functions can confront and act together on important issues. These opportunities are not sufficient to deal with the evolving speed of the environment in which the company operates and it is therefore necessary to use faster and always-active communication channels between the various departments. Otherwise, if a sector finds out an important change within its sphere of competence there will be a significant delay in transmitting and receiving information to and from other departments and core functions, resulting in a great loss of readiness and agility that makes almost impossible to act on time.
- **Loss of awareness:** the desire to protect core functions means that they have no direct perception of the environment in which the company operates, reducing or eliminating totally the possibility of developing their awareness and identifying and exploiting opportunities.
- **Loss of liability:** linked to the previous point there is another problem that arises from leading core functions into a certain and isolated environment. Core functions have to take important decisions based only on information filtered by other departments (those data may not be representative of reality) and without being able to directly track the developments and consequences of their actions. All this can be summarized

saying that core functions are no longer responsible for the long-term consequences of their choices, with all the issues that this may entail (unaware decision making process, short-sighted or contradictory choices, etc.).

- Safety stocks: as we repeatedly stated, one of the main objectives of a "silo structure" is to allow core functions to operate in a determined environment, even though the company itself lives in a context dominated by uncertainty. This choice is based on the will to have a stable and easily tuning environment, limiting as much as possible the use of substantive changes. To achieve such a situation, it is often necessary (in the case of manufacturing companies) to rely on large stocks of inbound and outbound resources, resulting in increased management costs and a general loss of efficiency. This is the classic case of a company that operates in a very variable and/or unpredictable market: the marketing department creates the demand forecast, indicating the large fluctuations of production volumes required in subsequent periods, at this point if the company may decides to act on their production capacity or to have to resort to large stocks of raw materials, semi-finished products or finished products to ensure that they can satisfy demand.
- Mistrust: in data coming from different departments due to the fact that lack of internal visibility prevents the different functions from having a perception of how the other processes works. A frequent example occurs when the production department receives the demand forecast created by the marketing sector. Maybe the previous forecasts made by marketing sector was imprecise (for example they may underrate the demand for several times) so the production manager may decide to arbitrary increase all the quantities by a percentage in order to "correct" these data. This should already represent a lack of control over the company and result in a reduction of efficiency (and maybe even effectiveness). This situation can become even worse if we consider the case in which marketing department has made some investment and improvements on its processes and tools in order to create more precise and reliable forecasts, then the production manager may be in the dark of that and continues to "correct" the data. Of course after some time the company will discover and solve this problem, but in the meantime it will have surely created some damages.
- Conflicting objectives: as we mentioned inside a "silo structure", the various departments act as autonomous units and each one has its own local objective. The problem arises when these local targets are no longer aligned with the company's overall goals (set by top management) or conflicting with each other, resulting not only in efficiency but sometimes also effectiveness loss. We can consider the example of choosing the optimal stock level to better clarify this problem. Both the production manager and the logistic manager may have the task of managing stock level. Production manager is interested in keeping a high level of stocks (of raw materials, semi-finished products or finished products) to conduct production operations in the most stable and smooth way possible despite demand fluctuations; logistic manager on the contrary will try to keep the level of stock as low as possible (as long as he can provide the required safety stocks) in order to keep logistic and warehouse management costs down. This is a perfect case of conflicting objectives and for sure this would result in an allocation of resources pushing in opposite directions (loss of efficiency), and without considering the problem from a broader perspective, it will not be possible to find a good tradeoff point (loss of effectiveness).

As we said at the beginning of this list all these problems share a common deep cause: inadequate internal communication management that can lead to two kinds of consequences.

Let's call the first the "**lack of vertical communication**" in which top management has a poor visibility of the enterprise structure reducing the awareness of what resources the company has and where they has been allocated and making the assignment of local goals and the tracking of their progress much more complicated (all this this may lead to situations like the one with conflicting objectives that we have described earlier).

We can define the second one as the "**lack of horizontal communication**" in which we have delays and missing communications between departments that create circumstances in which problems develop unnoticed, thus hampering risk management processes in all their phases (identification, analysis, mitigation, control).

Carol S. Switzer, OCEG co-founder and president, talking about the risk of heavily siloed approaches highlights the fact that critical information regarding risk and compliance operations are unable to reach strategic decision makers in a timely fashioned. In addition is not uncommon that inside a "silo structure" risk and compliance roles are seen as people who want to "put the brakes on" business decisions and therefore they are not included in strategic decision making meetings. This is one of the biggest mistake an organization can makes because they are significantly reducing the probability of taking successful decision since they are neglecting an entire set of information that is vital to take aware decisions.

Switzer continues listing other examples of the most common mistakes made inside a "silo structure": "Siloed operations spend too many resources trying to reconcile disparate information, have gaps and unnecessary overlaps in activities, put too much burden on the business by failing to coordinate schedules and requests for information, and even worse, may create new risks themselves."

At this point should be already clear that GRCs, which are based over the creation of a central information management system, represent a valid tool capable of solving the problems of "silo structures" by acting on the root causes.

4. PREREQUISITES FOR A SUCCESSFUL IMPLEMENTATION

This chapter is devoted to identify the requirements for a successful implementation of an integrated GRC system. Consulting the material available on the web (publications and interviews to experts and CEOs of companies) has emerged that the most determining factors for a successful and profitable implementation are related to the maturity of the company's risk management system. To develop this topic there have been identified 4 points:

1. Total and convinced **support of top management**.
2. Own and **use** a consolidated **risk management system**.
3. Conduct **proactive risk management**.
4. Develop the concept of **enterprise resilience**.

Points 1 and 2 represent the real essential requirements to be able to attempt the implementation, while others represent useful milestones for assessing the maturity of their risk management system and are factors that enable the systems to be used in a more profitable way (take full advantage of the potential of the new integrated GRC system and enabling the company to achieve the benefits mentioned in this document).

In the rest of the chapter, we will deal more in-depth with the various points, using as many industrial or secondary data as possible to clarify the importance and the advantages obtainable.

4.1 Top management support

Within a company, middle management has responsibilities and authority over the business sectors and responds directly to top management (senior management) composed of one or more figures (top manager, chairman, CEO, general manager, secretary-general, etc.), who has the responsibility and authority over the whole enterprise. Top management defines the direction of the organization and establishes the main milestones that represent the goals pursued by the middle management.

This document has repeatedly underlined the fact that such projects will engage large business resources for a long time and it is therefore necessary for top management to be fully convinced to undertake this path and become an active promoter in order to help the enterprise to hold the effort necessary during all the phases. The support of senior management is therefore the first and perhaps most important requirement for the simple implementation of the system (it is not enough, however, to ensure the correct use of GRCs and therefore to obtain the benefits offered), thus avoiding any rethinking during work that would result in huge costs.

Very often within the top management we can find the figures of the CEO and CIO that the authors of *Big Picture* identified as the figures who could participate in the choice of a GRC platform. They connect the two levels of management described above, bringing top management directives to the lowest business levels, and receiving from these last major feedback they will use to improve management and make proposals to be brought to the highest level of leadership. In fact they are the first corporate figures that propose to use these integrated tools to better align the results obtained from various business functions with the goals and directives of executives, and are also the users of Forrester's framework for calculating the ROI presented at the beginning of this document.

In chapter 5 we will see that top management may have a further role in helping the company during the implementation.

4.2 Risk management system

Nowadays in companies of all sizes, the risk management process is based on the systematic approach consisting of the following steps:

1. **Establish the context:** internal and external in which the company operates.
2. **Identification of risks:** which can affect the performances and achievements of company's objectives.
3. **Risk analysis / quantification:** characterizing them based on the likelihood of occurrence (possibly using statistical methods) and the severity of the consequences.
4. **Identification of causes.**
5. **Risk management:** identifying, where possible, interdependencies between risks and the possibility of exploiting synergies for a better use of resources. After an initial prioritization phase has been carried out, risks are processed, preferably by eliminating them or else implementing barriers to protect the system.
6. **Continuous monitoring:** of the identified risks, implemented barriers and periodic repetition of the identification phase in order to protect the system from new risks.

Companies nowadays use the so-called ERM, a collection of methods and processes to conduct risk management by following the steps outlined above.

However, the only fact that a company owns a risk management system does not automatically imply that it is used in the most proper way: if it is only seen as a tool to treat, for example, occupational safety or, as Switzer said, as a "brake" that obstacle other business functions, will be impossible for this precious tool to work properly and bring benefits to the company.

For this reason, one of the requirements needed to implement a GRC system is to "possess and USE a risk management system", meaning a conscious, widespread and in-depth use of risk management practices and tools. All this allows the company not only to protect itself more effectively, but also to gain awareness of its resources and potentials and to identify and exploit opportunities in order to get advantages over competitors.

In the following subchapters we will try to clarify what we mean by a "proper use" of the risk management system.

4.3 Proactive Risk Management

Risk management can be conducted in a reactive or proactive way. The first one concerns the investigation of an incident in which we are interested in reconstructing the facts and identify the causes of the event; the other one concerns process analysis and intervention on unwanted "outcomes" before they occur.

In the engineering field there are some proactive tools (FMEA and FMECA) initially used to identify and analyze the failure modes of a component or a system. The operation is straightforward and rigorous: once we have defined the element we are analyzing at the moment, we list all the ways in which it can fail and analyze each "failure mode" in a qualitative (FMEA) or also quantitative (FMECA) way and finally predict the effects (or outcomes) that they may have on subsequent components or the overall system. By doing so, it is possible to anticipate the problems and their consequences, acting in advance on the system and possibly putting barriers.

The strength of these tools (and proactive tools in general) lies in the fact that they are simply structured and rigorous procedures for analysis and treatment and can therefore be used in every field to treat the 4 types of risks identified in the so-called “4 risk quadrants”:

- Hazard risks: concern the risks to occupational safety and asset protection.
- Financial Risks: concern the risks related to monetary exchange (e.g.: € - \$), the fluctuation of energy, materials and products prices, loan fees, etc..
- Operational Risks: Customer Satisfaction, Product Success, Image Damage, Trade Unions, Supply Chain Management, etc..
- Strategic Risks: Product obsolescence, competitors behavior, product or market regulations, demand fluctuations, etc..

All this is nothing new compared to what companies are doing in their day-to-day operations, but it's important to understand the potential of proactive risk management so that a company can use these tools in the most profitable way and gain significant benefits.

An example might be the use of proactive techniques in the selection of suppliers: we can apply FMEA to analyze all the possible candidates to identify all the risks to which our company would be exposed in case it should depend by one or more of them.

In doing so, we will identify a number of risks (just like failure modes) such as:

- Risk of sanctions or embargoes (in the case of a supplier located in a country with particular arrangements or particularly uncertain conditions, e.g.: sanctions on Russia as a consequence of Ukrainian crisis).
- Risks deriving from regulations that are not compatible with those we have to comply: for example, materials or processes used by our suppliers. We recall the example of materials used by Mattel (presented in the previous chapter) that do not comply with US regulations or the case of some processes for working jeans fabric by use of (illegal) powders that are harmful to workers but are used anyway in some countries: in this case we can expose ourselves to sanctions or image damages.
- Risks related to natural disasters such as earthquakes or floods: depending on the location where we or our suppliers are operating, our supply chain may be exposed to potential disruption due to major events. An example of this may be to depend on suppliers or warehouses located in some areas of Southeast Asia particularly exposed to flood risk.
- Other supplier (and also customer) related risks. For example if one of our competitors is the main customer of one of our suppliers, they may have priority access to their production capacity, which could put us in critical positions in case we need to quickly buy extra capacity. At the end of this chapter will be presented the Nokia-Ericsson case where we will find this type of problem.

As we can see, depending on the single vendor we are assessing at the moment, we may be exposed to one or more of these types of risk, allowing us to make conscious choices and to implement the necessary protections. The normal supplier selection procedures might have ignored some of these risks, exposing our company to them and finding us probably unprepared to deal with them.

Hopefully this example will testify the potential of proactive and rigorous risk management techniques and the fact that they are in fact applicable to every business area, enabling the company to gain a good understanding of the risks, resources, and opportunities available.

4.3.1 Risk: threat or opportunity?

Some risk management techniques divides risks into two categories, based on the kind of consequences they may bring:

1. Pure (or static) risk: they can only damage the company, for example:
 - a. Risk of damage/loss of assets.
 - b. Risk for civil liability.
 - c. Occupational health and safety risks.
 - d. Risk of damage/loss of third party's assets of our company's responsibility.
2. Speculative (or neutral) risks: they can lead to both a profit or a loss to the company with a certain likelihood, so it enters the field closely related to the Operational Risk where the company evaluates scenarios and possible consequences to make strategic choices for the achievement of their goals. Here are some examples:
 - a. Market risks (e.g.: choosing to enter into a new market, the tendency of the customers to prefer online shop, being outmaneuvered by competitors, etc.).
 - b. Credit risks (e.g.: extending credit to customers).
 - c. Liquidity risks (e.g.: not being able to convert its own asset into cash).
 - d. Production risks (e.g.: production volume, managing stock level, etc.).
 - e. Political risks (e.g.: new/tighter regulations, sanctions, embargoes, etc.).
 - f. Risks of innovation (e.g.: choosing adequate level of product/process innovation, funding R&S, etc.).
 - g. Etc..

One of the methods developed to manage this type of risks is Operational Risk Management. The ORM considers the risk as a variation of performance that can be positive or negative; such variations are caused by uncertain events.

The only innovative element of this methodology is to consider the risk as a threat (negative variation of performance) or an opportunity (positive variation of performances) while keeping the two components of risk that we saw before: severity of consequences (became the extent of the variation, e.g.: the output of a process) and the probability of occurrence (here is the probability of occurrence of the uncertain event that causes the variation).

The consequences are quantifiable in terms of performance variation (e.g.: production capacity, lead time, number of nonconforming parts, etc.) or the value perceived by the stakeholders, thus including all the types of risks that we had previously identified.

At the end of this chapter will be presented the Nokia-Ericsson case and we will see how a series of timely choices (then revealed successful) have allowed one of these companies to turn a "category 1" risk (having only negative impacts over the company) in an opportunity for a huge growth and even for successfully wiping out the competitor from the market.

The purpose of this part in fact is to make aware that good management of any type of risk can lead to far more important benefits than simple protection, especially in a modern environment where the competitiveness between companies is fought on a huge number of fronts.

4.4 Enterprise resilience

BSI Group article titled "Resilience as a Value Driving Organization" begins with the phrase: "In an ever-changing complex market, more and more people talk about resilience. Resilient organization not only survives, but is able to anticipate, be prepared and respond appropriately to change, seizing opportunities in order to thrive in a dynamic environment."

and defines corporate resilience as follows: "Resilience goes beyond the concept of mere risk management, defining a more holistic vision of long-term business success as the value that drives the organization."

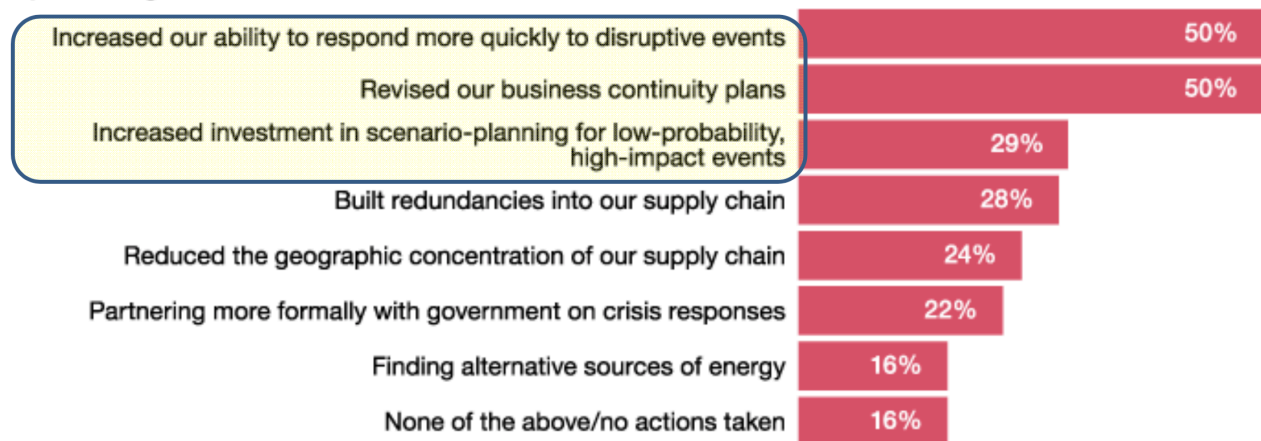
To better define the concept, we can group under the name "enterprise resilience" all business procedures that enable the company to improve: capitalization of experience, innovation, risk management, and maintenance of business continuity.

APEC conducted a research interviewing some CEOs of companies that were directly or indirectly damaged by the March 2011 Japanese earthquake and tsunami to gather testimonies of the lessons learned from that event. The following picture shows some of the conclusions reached by the study and in particular the most frequent responses of the CEOs that claimed to suffered huge damages.

Lessons learned for CEOs: respond quickly...then reset risk management approaches

[Following the March 2011 Japanese earthquake and tsunami] which of the following actions, if any, did you complete as a result?

Those who responded to a prior survey question stating their business was impacted 'to a great extent' or 'to some extent.'



PwC, 2011 APEC CEO Survey, November 2011

Figure 10: Conclusions of the APEC CEO Survey (Source: APEC)

As we can see the three main answers about the lessons learned and the initiatives created to react are:

1. Increased our ability to respond more quickly to disruptive events.
2. Revised our business continuity plans.
3. Increased investment in scenario-planning for low-probability, high-impact events.

Here we find perhaps the most important and critical part of corporate resilience: sometimes is not easy to justify investments in some of these areas (such as low-probability scenario analysis, in response 3) until we experience a similar event; we may understand such a choice but "in a constantly evolving market" (BSI Group) like this one, just one severe disruption may be sufficient to kill a company preventing it from surviving and learning from that event. In this regard, we can quote the sentence: "If you think Risk Management is expensive, try an accident."

One of the areas where various experts are focusing on is the creation of tools similar to the Forrester framework for calculating a GRC's ROI to help managers in justifying investments in business resilience processes highlighting how these can bring benefits also to day-to-day operations.

Let's start by presenting the phases that allow the company to deal with a disruption while maintaining stability and minimizing the recovery time (for each we will show examples of how the processes created to respond to emergencies can bring benefits to the company also during normal operating conditions):

1. **Sense:** the set of business features that allow the company to identify and memorize, from past experiences, the knowledge to identify useful KPIs (required for monitoring) and to be able to properly spot and interpret the "symptoms" of events that are going to happen or that have already happened but whose consequences are not fully manifested yet. Under normal circumstances, it enables the company to capitalize the its knowledge and to facilitate the creation of manuals and staff training programs.
2. **Build:** the set of functions devoted to the proactive creation of skills that can be used proactively or reactively, and to study and experimenting new reconfigurations of the existing assets in order to react quickly and effectively. These processes are based on creating skills that are useful to the company and therefore contribute to more efficient and effective staff management.
3. **Reconfigure:** the set of functions dedicated to improve company ability to adapt to changes with multiple forms of flexibility in order to easily deal with a disruption or simply adapt better to the conditions in which it is operating (evolutionary optics). It is obvious that a company's ability to be flexible allows it to gain significant benefits also in day-to-day operations: launching new products or managing modest fluctuations in demand will require limited time and resources.
4. **Sustain:** the set of functions dedicated to ensuring the business continuity during recovery time, reducing the time needed to recover from the consequences of a disruption, reducing and preventing long-term consequences, and acquiring knowledge and skills for future use. These processes also contribute to the capitalization of corporate knowledge, with the advantages we have already identified.
5. **Re-enhance:** the set of functions designed to take the actions needed to recover from a disruption and at the same time exploit the opportunities that may result from them. This function seems to be totally tied to emergency management, but it basically aggregates all the capabilities that allow a company to plan and make important changes that require long implementation time, allowing it to undertake more important and challenging development projects.

The following picture shows a graphical representation of the various phases since the time in which the disrupting event occurred until the restoration normal operating conditions (which may be different from the initial ones).

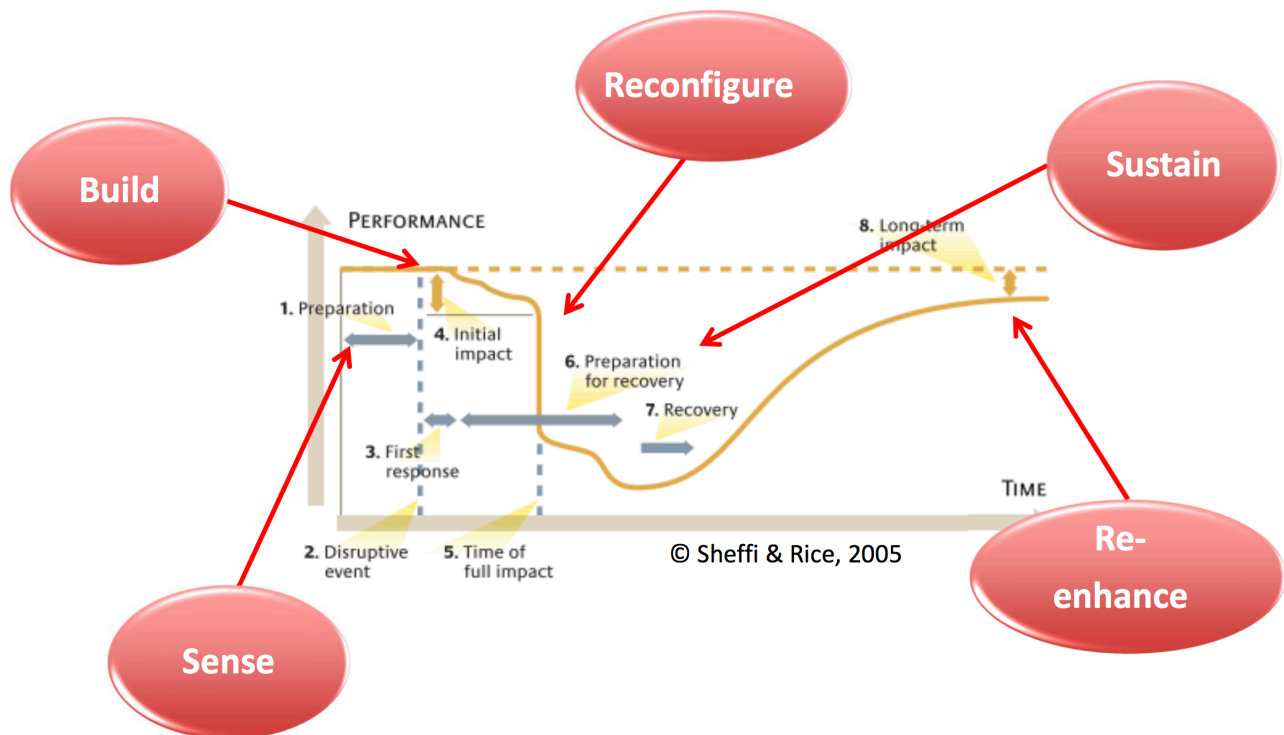


Figure 11: Representation of the phases and the action made by a company from the time a disruptive event happens until the restoration of normal operating conditions (Source: Sheffi & Rice)

The picture represents the life of a company as a cyclical succession of (more or less serious) disruption from which the company recovers, so we can think that before “time 0” of this graph the company has suffered a disruption, has managed to react and recover, has gained some precious knowledge and now the cycle is about to restart again with a new disrupting event.

The first phase, marked as "preparation", can therefore be about the time interval between the restoration of normal working conditions after the end of a previous disruption and the new "disruptive event". However there could be another way to interpret this graph: the “preparation” phase could also be seen as the time in which the company was collecting, analyzing and cataloging experiences in order to gain knowledge to be used for continuous improvement of its processes.

In this phase the “Sense” function determines the company's effectiveness in capitalizing on its know-how and experience; its second task is to monitor a set of KPIs that allow the company to minimize the time between the occurrence of the disruptive event and the time in which it is identified; in some situation the disruptive event may even be even anticipated, identifying the warning signs and initial symptoms.

The “Build” function comes into play from the time the company becomes aware of the disruption and has the task of selecting and organizing the skills needed to react, usually this phase involves the creation of task forces designed to predict all the possible consequences of the disruption and elaborate the necessary strategies.

Meanwhile, the consequences of the event are reducing the performance of the company and during the “Reconfigure” phase the main concern is to wage the resources needed to adapt and to be prepared to respond as quickly as possible.

At this point (“Sustain” function comes into play), the recovery phase starts and the first concern is to sustain the effort of the company without risking dispersing energy and resources into unnecessary processes.

Once the emergency is over, there will be a period of time during which the company recovers until the restoration of normal operating conditions which may be different from the initial ones (as we will see in Nokia-Ericsson case a company may even improve its initial performances if able to manage properly a disruption).

During the final phase “Re-enhance” function has the task of gathering and analyzing data and lesson learned by this experience in order to decide whether to restore the functions and procedures already in place or to take advantage of this transition phase and make changes to increase its effectiveness and efficiency.

The cycle ends by transferring this knowledge to the “Sense” function in order to be integrated into the corporate cultural heritage for future use.

As we have seen all the functions that have come into play can be used both in a reactive way, to deal with a disruption, or proactively, in order to increase company’s awareness of its own resources and the external environment in which it operates, allowing them to have a continuous and harmonious process of learning, gaining competitor advantages and improving their own risk management and emergency management system.

GRC systems seem to be very harmonious within this philosophy, facilitating the transfer of information within the company and all its components, enabling it to make full use of all the data and experiences gathered in order to increase its resilience and proactive processes.

4.5 Nokia-Ericsson Case

To conclude the discussion on risk and emergencies management will now be presented the Nokia-Ericsson case. Here we will find an example of the importance of correctly capturing and evaluating the information, the importance of internal communication and how it is possible to turn a negative event into a precious growth opportunity (via a proper understanding of scenarios and timely planning and execution).

4.5.1 The disruption

On March 17, 2000, a Philips semiconductor factory located in Albuquerque (New Mexico) caught fire. The security measures proved to be effective (sprinklers and Philips-trained staff successfully managed the situation), the fire was tamed and once the firefighters arrived to the scene they just had to decree the end of the emergency.

Philips estimated the total cost related to this disruption as the combination of the costs needed to replace damaged lots and the penalties for having failed to comply with the delivery deadlines.

This plant supplied both Nokia and Ericsson and Philips announced to both a one-week delay for the subsequent component shipment.

The problem was that despite the fact that the fire had developed in the furnace area, it had triggered a number of consequences that affected the whole plant. Microprocessor manufacturing plants require closed space provided with an air filter system capable of intercepting any particles larger than 1 µm in order to prevent dust deposits on silicon wafers and guarantee their quality.

The fire had irretrievably compromised the controlled atmosphere of the factory due to smoke and the passage of personnel and firefighters “contaminated” by dust and soot.

The result was that all components, semi-finished products and finished products located in the plant were irrecoverable and the estimated time needed for restoring normal operating conditions went from a couple of weeks to several months.

Let's see now what happened inside the two companies after receiving the news of a one week delay (this kind of situation was fairly common in that type of industry and thus easily manageable using safety stocks).

4.5.2 Nokia response

After receiving the call from Philips, Nokia Chief Component-purchasing manager, although not particularly worried by that news, informed other company members, including Nokia's chief troubleshooter, who felt that the situation, not alarming at the moment, required closer observation.

Nokia activated a "pre-emergency" plan, creating a list of the components produced in that plant, monitoring the situation with daily phone calls and offering to send engineers to speed up recovery operations.

Two weeks later, Nokia received from Philips the communication of the actual extent of the damage and established immediately a task force of engineers and supply managers to create an emergency plan in order to being able to purchase the required components elsewhere.

At the end only two components were impossible to be procured by other suppliers, so Nokia had a face-to-face meeting with Philips asking to have access to detailed information about the production capacity of their remaining plants and to use that capacity to produce those parts; for a short period the two companies operated as one entity.

With this huge and timely effort, Nokia was able to successfully manage the emergency and reducing negative consequences to the minimum.

4.5.3 Ericsson response

Ericsson received the same communication by Philips about the one-week delay of the subsequent shipment but considered it as acceptable and, even when they were running out of critical components, low-level employees had not yet informed their managers.

When Ericsson realized the real gravity of the situation it was already too late: Philips' and others suppliers' extra capacity was already "taken" by Nokia, leaving Ericsson with few chances of containing the damages.

4.5.4 The results and lessons learned

The results of this series of events were catastrophic for Ericsson, which was short of millions of key components for the manufacture of a new generation of phones that was about to launch on the market and found itself with an inadequate mix of products.

The economic loss for them was about \$ 2.3 billion, and after one year the decision to shut down the phone industry led to the creation of Sony-Ericsson, a 50-50 joint venture managed by the two companies.

For Nokia, however, what initially could be a disaster with similar consequences turned out to be an opportunity to eliminate the main rival from the market and earn 3% of the market share in just 12 months, all thanks to their more aggressive and proactive business culture.

Analysts studied this case with great curiosity and found in Nokia a great awareness of the true value of information flow within a company.

Indeed, regardless of what may be the opinion of the person who first receives a news, business policy requires a high level of internal communication so that those information can reach the people with the right skills needed to make the best use of them.

In the case we just seen, it was the same Nokia manager who, despite not considering the situation particularly alarming, forwarded the information to the rest of the company by putting in motion various processes, so that those apparently ordinary news could reach the troubleshooter.

A statement from Nokia's troubleshooter was: "We encourage bad news to travel fast, we don't want to hide the problems"; we can find these principles in all the systems that stand out for readiness and effectiveness in identifying and solving problems.

Once again, we can reiterate the fact that the centralized information management system created by GRC systems is perfectly aligned with Nokia's strategy and with the philosophy of sharing information and competences inside a company in order to act as one entity against problems.

4.6 Conclusions

Finally, we can summarize what has been said in this chapter by briefly recap the steps a company should take to make its own risk management system mature and ready to support a successful implementation of an integrated GRC system and increase the probability to make a profitable use of the new system.

The first step requires the creation of an ERM system based on an advanced and aware risk culture (knowing the value of the information and the benefits that can be obtained) to use all the tools and methodologies available in an integrated and complementary way.

The second step involves the creation of proactive management processes to establish the barriers necessary to protect the company against risks.

The last step is related to the creation of processes and tools needed to monitor the company, both internally and externally, to identify all the indicators (KPIs) useful to create a dashboard capable to spot all variations and quickly activate the risk and emergency management system, in other words, the creation and development of their enterprise resilience.

5. GUIDELINES FOR A SUCCESSFUL IMPLEMENTATION

This chapter is dedicated to supporting the implementation phase of the integrated GRC platform by suggesting procedures that may not be identified during the design phase.

The reference materials for this parts are articles written by consulting companies and interviews to top managers of companies that have successfully accomplished the installation phase of an integrated GRC system and are making a continuous and profitable use of it.

In order to provide suggestions for easing the implementation phase and to allow the company to create the conditions to take advantage of the full potential of the new system, the authors of this document identified the following points:

- Being able to communicate the reasons for the adoption of a GRC system and motivate the staff.
- Creating a common language.
- Basic training on risk management.
- Active staff participation during the design stage.
- Handle the project in phases.

We will now provide a more detailed description of the various points.

5.1 Motivating and communicating the reasons

Several times during this work has been highlighted the fact that GRC systems involve all corporate functions and staff at all levels in a common effort.

As we said usually is the CEO the first who takes into consideration the adoption of an integrated GRC system to improve the performances of the company and to solve some of its problems coming out during day-to-day operations.

At this point, after having evaluated several alternatives and selected one or two platforms, he brings the proposal to the corporate council in order to take a choice. As we have pointed out in the previous chapter, is absolutely necessary that top management is fully convinced of willing to undertake this project and becomes an active supporter and promoter of it.

Now we can get in more detail of how top management can concretely support the implementation phase. In fact low-level staff is the one who will use the new system and deal with new procedures and tools sometimes very different from those he was accustomed to.

This certainly implies a significant effort on their part so it is crucial to motivate them and to make them feel part of this project. One way of doing this is to make them understand the motivations that led to the choice of using the GRC system and the benefits it can bring to them and to the entire company.

It is therefore intended to make them perceive the adoption of an integrated GRC system not as something imposed from above (and to which they just have to adapt), but as something that can give a positive contribution and that requires their work in order to be able to do so. In other words, it is about meeting each other: the GRCs help us to solve some problems and gain benefits, in exchange we, as a company, help GRCs to function properly by leaving the comfort of our old procedures and embracing new ones.

As we know motivation is by far the most critical and difficult to manage variable of project management, and become even more important in case (such as this) in which the way staff perceives the project will have heavy consequences not only on the success of the

implementation phase but also on how the new system will be used during day-to-day operations.

We will understand better this topic in point 4, showing another way of motivating the staff to interact in a proper way with the new GRC system.

5.2 Creating a common language

It is not unusual that within the same company, different departments or functions use the same terms with different meanings.

This could be tolerated without any particular problems within a more fragmented structure (silo structure), but given that GRCs intend to create a centralized information management system to which all departments will have access, it is essential to create a single and standardized vocabulary and make sure that the entire company adopts it.

This point might seem trivial, but if left over, it could lead to many problems in the early stages after implementation, when staff will start to interact more and more frequently with the system.

In fact, as we said, one of the purposes of the centralized information management system is to analyze data to support the decision-making process, so without a common language those information will become incompatible with each others, or in the worse case they could lead to misunderstanding and poor decisions.

5.3 Basic training on risk management

As mentioned in the beginning of this document, the "Risk" part of GRC systems seeks to make risk management a component of all the processes of the company.

This does not necessarily mean that the company should give up having a "centralized" or "unique" risk management function in order to reach a condition in which each department manages its own risks.

Such a situation, in addition to being difficult to achieve, would prevent the company from having an overview of the entire organization and managing risks in a more coordinated way, thus not being able to exploit possible synergies and risking to lose efficiency and effectiveness.

A better way would be to provide at least basic training to personnel in charge of interacting with the centralized information management system so that they can identify all the information useful for risk management (for example knowing the importance of the so-called "voluntary reports" of which we will discuss in the last chapter when talking about the so called "Just Culture").

Thus risk management could still be carried out by a dedicated function within the company, which could rely on a desirably more complete and constant stream of valuable information.

Choosing to train only the staff responsible for interfacing with the information system is an acceptable compromise; the most ideal scenario would be to extend the training to all staff, but it may be ineffective as well as expensive.

What we just said is valid also for the Compliance part of GRCs; a company may decide to train the staff also for compliance management if it is a particularly critical element of its business.

5.4 Active staff participation

One of the major problems for a company that invests in such an important system as a GRC occurs when, after implementation phase, staff shows some resistance in using it, risking to making all the efforts and investments vain.

The risk is to be unable to take full advantage of the new system and at the same time to see the creation of other communication channels preferred by the staff.

The first step should be the determination of the possible causes that lead to such situations; we can list some of them:

- a. Particularly complicated system interface and non “user friendly” processes, maybe caused by errors made during the design phase.
- b. Inadequate training on how to use the system as a result of problems during the training phase.
- c. A distrust in new systems, as a result of a failure in motivating the staff.
- d. A perceived ambiguity in the company's behavior, the staff might perceives a lack of confidence by company (usually top management) in the new system and feeling less motivated to use it, in this case the management's support might have failed.

The company may try to solve some or (hopefully) all of these problems by choosing to actively involve the staff in the design phase of the new centralized information management system they will be asked to use.

Collaborating to the creation of the audit structure or system interface could eliminate the risk of creating program too complicated to use (point "a.") and consequently problems during the training phase (point "b.") would be easily solved/prevented.

Being personally involved means that staff is more motivated and willing to use the system that he contributed to create.

This is one of the best ways to increase not only the probability to successfully complete the implementation phase, but above all creates the conditions to use the GRCs in a more aware and profitable way, maximizing the benefits obtainable and justifying the investment.

5.5 Handle the project in phases

This last point concerns a practical suggestion that is strictly related to project management.

Companies that have implemented a GRC system suggest to proceed one sector at a time, integrating it into the system, and then moving on to the next one, in order to be able to carry out the project more easily and at the same time maintain continuity in operations.

This suggestion assumes that the company is making a transition from a "silo structure" to an integrated structure built around the new centralized information management system that represent the backbone of the new configuration.

This final structure does not necessarily intend to eliminate the departments, but it is necessary to break down the “walls” which, in the "silo structure”, isolate the various functions; this is mainly done by the Governance function of the new integrated GRC system via the creation of the centralized information management system.

These suggestions should help and support the company during the implementation phase, however it is not possible to identify the exact moment in which it is accomplished because the organization has just begun the path to reach what OCEG calls “Advanced GRC”. In other word this is the condition in which the integrated GRC system reaches its maturity, the

company has managed to become fully confident in using it and has “refined” all the processes in order to make them effective and efficient.

In the appendix will be provided an image that should be able to give an idea of the main phases in which a company should go through in order to reach the conditions we just present.

Unfortunately, the material available in this regard is not sufficient to properly treat it in this document. In fact, usually companies deals with these phases in an unstructured way, making almost impossible to identify the set of steps that contributes to the creation of an “Advanced GRC”.

The good thing is that, considering the fact that the material about the implementation phase and its prerequisites is relatively new and is continuing to grow, we may expect that in the future more and more information will become available, allowing to collect and share useful guidelines to increase the knowledge and the awareness also on this topic.

However what we can do at the moment is provide some suggestion about management techniques or tools capable supporting and completing an integrated GRC system taking advantage of some common points and synergies. The following chapter is therefore devoted to address this topic.

6. SUGGESTIONS FOR FUTURE DEVELOPMENT

This last chapter intends to provide suggestions to continue the improvement path that the company has undertaken with the implementation of the GRC and its use during day-to-day operations.

For this reason, two management techniques perfectly aligned with the philosophy and modus operandi of integrated GRC systems have been selected and can therefore be implemented in a particularly easy way and make important contributions to both the GRC system and the enterprise.

We will present:

- The BYOD (Bring Your Own Device) policy.
- The “Just Culture”.

6.1 BYOD Policy

In recent years, the market of personal devices (smartphones, tablets, PCs, notebooks, etc.) has radically changed by incorporating more and more features and allowing better interconnection.

This has led to the development of policies and management techniques that allow the use of personal devices also for enterprise applications, with the aim of responding both to the demand of the staff to be able to use their own devices and the need of the company to reduce equipment purchase costs.

The use of these policies allows for increased productivity (mainly linked to faster response times as employees become more familiar with their devices) and the guarantee of an adequate level of protection of sensitive company data by external attacks or violations.

Usually, within a company, IT department is in charge of dealing with device management and data security, and in order to do so can choose to act at multiple levels:

- MAM (Mobile Application Management) includes a set of software practices that allow the company to create and manage their own app directly, allowing the employee to have the privileges of accessing enterprise systems from their device. In this case, the company may perform various actions such as obligatory update of the app to make everyone use the same version of the system at the same time and revoke access rights in case of termination of the employment relationship. It is typically used to handle the devices of company’s representatives and sellers who need to move freely on the territory.
- MDM (Mobile Device Management) allows the company to control all devices that have the right to access the corporate network. This requires the interaction of two components: an internal server (which sends the commands) and an element internal to the device (which receives and executes them). This is the same procedure used to allow users to download and install operating system updates on their devices without the need to connect to a computer.
- MEM (Mobile Expense Management) enables the company to use software to collect information about mobile device expense. In this way, it is possible to have a comprehensive cost control (by distinguishing the costs between voice and data traffic for business use and the one for personal use charged by the individual employee) in order to choose the most appropriate type of contract for their needs. It is also particularly useful for assessing the use of personal devices inside a company that intends to choose the most appropriate management strategy (e.g.: MAM or MDM).

The choice of using and managing personal devices for business purposes, however, is very challenging for IT department, which has to operate in situations of great complexity.

In fact, if we try to look at the personal devices of a company's employees we would not only find a variety of brands (LG, Apple, Huawei, etc.) and operating systems (Android, iOS), but also the coexistence of different models (iPhone 4S, iPhone 5, iPhone 6, etc.) and different versions of the same operating system (in fact not everyone upgrade their devices at the same time).

Knowing that, if we try to look again at the two main advantages identified before, we understand that although an increase in productivity would be very likely achieved, reduction cost is a different story. In fact, while the company saves on purchasing the devices to be provided to employees, the IT department will need better tools and resources to properly manage its tasks and to guarantee the adequate level of data security and the protection of both the employees and the company.

If we apply BYOD policies into an existing integrated GRC system, it is clear that an easier and faster access to the centralized information management system allows the overall system to be more responsive and at the same time motivates and involves the staff in using it, thus broadening the amount of data it can receive, analyze and make available.

6.2 Just Culture

This subchapter intends to present the so called "Just Culture", a concept coming from the aeronautical domain (related to management of aviation safety) based on the fact that one of the key factors for accident prevention is the risk management culture and the possibility to count on (as large as possible) set of information on which to build the process of risk management.

To introduce the discussion on this topic we are going to provide a part of the article "Trasporto aereo. Imparare dagli errori. Ecco cos'è la just culture" (In English: "Air Transport. Learn From Errors. Here is the Just Culture") by Patrizio Paolinelli (Wordpress); this article is particularly helpful not only to present what "Just Culture" is, but above all it tries to explain why it is so important to bring it IN OUR COUNTRY and facilitate its diffusion.

"Just Culture is a concept born in the Anglo-Saxon world that brings together a number of practices and attitudes regarding security in high-risk environments. This is an approach aimed at prevention and for what concerns air traffic management it overturns our approach to address daily problems. Too often in Italy the occurrence of inconveniences or, even worse, aviation accidents triggers a kind of manhunt. Once the person to blame is identified and condemned, INjustice has been done because everything remains more or less the same as before and the root causes of the problem has not been addressed. This modus operandi is based on the "Blame Culture" and consists essentially in the pursuit of a scapegoat. This pursuit always ends up finding a sacrificial victim, ignoring the responsibilities of the organization, and failing to take full advantage of the information. Paradoxically, what appears to be a strongly punitive approach is in fact largely exculpatory. But, controversy aside, what's worse is that as an invisible cloak the guilty mentality influences the day-to-day operation of flight controllers even when anomalies or errors do not have a negative impact. "

From these few lines the author wants to make us understand how the blind will to find and punish the guilty can lead to the loss of the opportunity to prevent other similar accidents.

A superficial vision might conclude that this would mean that those who are responsible could remain unpunished and free of consequences for the sake of preventing other negative events, but in reality it's exactly the opposite.

Like the author said a well-conducted investigation does not only lead to identify the root causes of the event but also the true responsables (instead of looking for what the author defines as scapegoats) so we don't have to give up justice to prevent new accidents but we can get benefits on both sides.

6.2.1 Linate accident, October 8, 2001

National Geographic has created a series of documentaries called "Air Crash Investigations" (in Italian "Indagini ad alta quota") that shows (through detailed reconstructions, archive footage and actors) the investigation of aerial accidents.

In the episode dedicated to the Linate accident of October 8, 2001, we can see that when the ANSV chief investigator arrives on the scene he was prevented to proceed by local law enforcement for few hours and the narrator of the National Geographic (thus providing an "international" point of view) explains that: "Unlike many countries, Italy considers aircraft accidents as crimes, so law enforcement has the lead of the investigation."

If we think about it we can easily imagine that local law enforcement are totally unprepared to investigate an aircraft accident because the complexity of the event and the airplane that would require a wide set of specific competences in order to know what are the relevant clues and how to proceed.

The best way we can imagine to deal with a situation like that would be to inspire a reciprocal cooperation between the two parties, to assist the knowledge of ANSV detectives with the workforce of local law enforcement.

Unfortunately what happened is that the ANSV detectives has to wait several hour before they was authorized to enter the accident scene and at that point a lot of relevant clues had already gone lost.

However, despite the lost information, it was still possible to reconstruct the true series of events that led to the incident, identify the root causes and make the necessary changes to Linate Airport.

This brief excursus had two aims: providing an example of the problems related to what we can define "a blind pursuit of justice" (in a very complex and critical system such as aviation is easier to see it but as we will show later also in industrial field we can get benefits from applying the principles of Just Culture) and to provide the background to the conclusions reached by the ANSV investigators that, how we will see, are nothing but the symptoms of a "corrupted" risk management culture and can be found almost in every sector, not only aviation.

The investigators discovered two shocking things:

1. Staff had become accustomed to the lack of appropriate tools (the radar ground was stored in the warehouse but never installed, sensors has been permanently disabled to avoid false alarms, navigation signage was unreadable, etc.).
2. The staff had become accustomed to a variety of "near misses", events that were about to become accidents but were avoided at the last moment mostly by chance. In fact less than 24 hours before a very same accident was about to happen on that same runway, but the collision was avoided at last thanks to pilots' promptness, favorable weather condition (they had good visibility, on October 8 instead there was a dense fog with very poor visibility) and a large dose of "good fortune".

6.2.2 Risk management culture

These problems are the consequences of wrong risk management culture and may be seen in any other situation; in fact also during our daily life we may act in this way. For example if we climb on a ladder to clean a high shelf we can decide to "take the risk" of leaning from the ladder in order to reach a far shelf without "wasting time" to move the ladder. Then if we risk falling but at the end (luckily) nothing happens we experience a "near miss" event and have the opportunity to decide how to use that experience.

We may decide to ignore that event and to take again that same risk or modify our behavior in order to reach a higher level of protection.

This example might seem trivial but could be useful to understand how easy is to become accustomed to take always the same risk (ignoring warnings) until something goes wrong and how crucial is to develop the risk management system based on a "healthy" risk culture.

6.2.3 How Just Culture works

Just Culture acts right on the culture of risk management, seeking to improve internal communication to help gather and analyze important data.

The main pillars of Just Culture are the creation of a spirit of collaboration and mutual trust between all hierarchical levels of the organization and the awareness of the importance and effectiveness of prevention.

The first thing to do is to make clear and structured the risk management and its procedures with the support of regulatory guidelines and other resources, so that the entire organization can align its efforts and objectives in order to improve its risk oversight and effectiveness in prevention, protection and reliability of its systems.

The entire company is therefore acting together to continuously improving its risk management processes, gathering precious information from lower-level staff (the one that can reports all the issues encountered during day-to-day operations) and using them to integrate existing procedures and training programs or creating new and more effective ones, all according to the "learning culture" that we already encountered during our discussion about enterprise resilience.

By doing so, also if the individual worker is facing a new situation is not alone but can count on a series of instructions and guidelines provided by the company and created also thanks to his contribution.

In order to create the conditions necessary to put in place these processes the company needs to encourage as much as possible the collection of voluntary reports (those considered not mandatory by the regulations) that usually concern the "near misses" events we mentioned earlier or any minor problem or failure encountered during normal operations or maintenance.

In some particularly complex sectors such as aeronautics or other business characterized by the interconnection of different systems, procedures and competences, is very difficult to carry out an effective proactive management capable of identifying (ideally) all the risks.

It is therefore essential to be able to count on a set of data as wide as possible, that could provide vital information for protection and prevention, especially because we could encounter minor events that highlights some criticalities that, in other conditions, may lead to serious consequences (as we seen for Linate accident, the "near miss" event of the previous day could has saved a hundred of lives if managed properly).

This “treasure” of information, although we have started considering the aeronautical field for its particular characteristics, is starting to raise an ever-growing interest in other sectors and will be most likely adopted in the industrial field in few years.

In fact even in this sector, we have always more and more examples of particularly complex systems (power plants, oil platforms, state-of-the-art facilities, etc.) and companies aiming to continuously improve their proactive risk management in order to gain a number of advantages:

- Better protection against the risks of a disruption;
- Lower costs for the consequences of accidents;
- Less risks / legal costs;
- Better insurance conditions;
- A more robust risk profile that increases the attractiveness perceived by potential partners, investors or buyers;
- Etc..

It's not a coincidence that we keep encountering more or less the same kind of benefits when talking about GRCs, enterprise resilience, proactive risk management, Just Culture, but is a proof that they are all aligned and share common goals, collaborating and integrating each others.

6.2.4 Creating the necessary conditions

Let's now give a look to what is needed to create the conditions necessary for establishing a voluntary reporting system.

Everything is based on the mutual trust between the one that makes the voluntary report (usually lower-level staff) and the organization: as we have said, the event may be an anomaly or the result of a mistake caused (then blocked before it would have any particular consequences) by the one that now is reporting it to the company.

In fact, although these data are entered in the system following precise procedures to protect the privacy of the people involved (personal information are removed, but general information are used to classify and analyze the event; for examples the report describing for example the role of the people involved: e.g.: pilot, mechanic, etc.; the type of system: airplane X, machine Y, etc.), it may be still possible to identify the people mentioned.

For example, if we consider a small airline in which only two pilots are trained and assigned to pilot aircraft XY or a small company where there is only one milling machine. We understand that if the report is about a “near miss” event happened to the aircraft XY or a milling machine, it would be straightforward to trace who might have committed and “anonymously confessed” the mistake.

Apart from the case of abuse, malicious intent or serious negligence attributable to an individual who will be properly prosecuted, the sole way to use these voluntary reports is and must be an anonymous and aggregated analysis for risk management purposes.

Here is where mutual trust comes into play and it is precisely here that we reconnect to what we, and Paolinelli, meant by saying that applying it in our country is very difficult.

As Paolinelli highlighted, Just Culture was born in a British context and has been successfully transposed in the countries of northern Europe, just for the reasons we can list here:

- voluntary data are valuable for proactive risk management and can therefore help save lives (prevent accidents even if we are dealing with occupational health and safety);
- Just Culture helps identifying the root causes and attribute real responsibilities to all those involved;
- doing this does not mean leaving the "guilty" unpunished (we already know that people guilty of abuse, malicious intent, or serious negligence are prosecuted and punished).

If we are able to absorb these concepts into our culture we could get all the benefits that we have highlighted and at the same time increase the possibility to identify and punish the real guilty rather than the scapegoats.

Just Culture requires that the company or anyone else should not be able to pursue the employee in any way unless he falls into one of those serious cases, listed previously.

Nowadays, in Italy, even if a company tries to create this mutual trust between all its hierarchical levels and gather voluntary reports, we can be quite sure that, without laws capable to understand the true potentiality of these principles and protect them, if an accident should happen the judiciary would compromise that mutual trust by misusing voluntary data.

Maybe all we can do for now is spreading the knowledge of techniques such as Just Culture in order to open the way for improvement and asking for the support of regulatory bodies and institutions.

6.2.5 What Just Culture can makes for integrated GRC systems

As we have pointed out several times during this work, the GRCs require a number of changes to the company, including some cultural ones, so we believe that they represent a great opportunity to begin a change that is becoming more and more necessary.

In doing so, it could also open the door to the introduction of Just Culture and other innovations that require a difficult and long-lasting cultural evolution.

To conclude this discussion we can list some of the expected benefits deriving from the introduction of Just Culture within an integrated GRC system:

- The foundations of Just Culture can support and promote better use of the GRC information system by introducing the volunteer reporting and analysis components regarding not only risk management but also compliance and hopefully any other area promoting the importance of non-compulsory reports.
- Just Culture philosophy is very aligned and can somehow complete the way in which GRCs are going to conduct risk management: support the proactive risk management with a wider database.
- Collaboration and mutual trust between the various business levels is something that we have already suggested to implement and exploit during the implementation phase, which could thus represent a starting point for creating the conditions necessary to adopt the Just Culture.

7. CONCLUSIONS

We hope that this work has been able to provide ideas and information useful to clarify the main aspects of GRC systems and their implementation and can therefore serve as a starting point to allow companies to deepen the elements most interesting for their business reality.

One of the ways to continue this “preparatory work” could be the creation of other complementary studies, each one focused on one of the topics, here addressed only superficially, in order to create a set of documents capable of helping the companies in dealing with specific problems and needs. In this optics this document could become the fulcrum of this project, introducing and connecting all the others works.

In our opinion one of the most interesting topic is about the identifications and study of other management techniques and tools and how they can interact or enrich an integrated GRC system. This would allow the identification of useful and valuables synergies that may bring great benefits to companies interested in using and supporting an integrated GRC system.

In fact, even if in this document has been selected only the BYOD policy and Just Culture, this is just the tip of the iceberg of such an interesting topic.

BIBLIOGRAPHY

- (n.d.). Retrieved from <http://www.tapestrynetworks.com/issues/corporate-governance/risk-management-and-oversight.cfm>
- (OCEG), O. C. (2009). *GRC Capability Model "Red Book" 2.0*.
- 1.27-1.29, I. t. (n.d.). *theinstitute.org*. Retrieved from <https://www.theinstitutes.org/comet/programs/arm/assets/arm54-chapter.pdf>
- Aaker, D. (n.d.). Retrieved from Prophet.com: <https://www.prophet.com/thinking/2016/02/256-silo-saboteur-the-organizational-structure-destroying-your-brand-strategy/>
- Anil Suri, P. (n.d.). Vice President and Chief Risk and Audit Officer, Pacific Gas and Electric Company. *Governance, Risk Management, and Compliance: Creating the Right GRC Strategy for Your Company*. ExecBlueprints.
- Association, W. A. (n.d.). 3C's Model (3C analysis business model).
- Banham, R. (2007, 6 1). *Is ERM GRC? Or viceversa?* Retrieved from TreasuryandRisk: <http://www.treasuryandrisk.com/2007/06/01/is-erm-grc-or-vice-versa->
- Barbara Monda, P. d. (n.d.). The effects if Enterprise Risk Management adoption on firms' value and performances: an empirical analysis using structural equation modelling.
- Benegal, B. (n.d.). Retrieved from IdmWorks.com: <http://www.idmworks.com/breaking-silos-network-security-using-grc/>
- Boldrini, N. (2010, 07 07). *Governance, risk and compliance: a passi lenti verso l'integrazione*. Retrieved from ZeroUno: http://www.zerounoweb.it/osservatori/securityjournal/governance_risk_and_compliance_a_pabi_lenti_verso_integrazione.html
- Cervelli, R. (2012, 01 26). *Governance, Risk e Compliance: un framework per calcolarne il Roi*. Retrieved from ZeroUno: <http://www.zerounoweb.it/osservatori/securityjournal/governance-risk-e-compliance-un-framework-per-calcolarne-il-roi.html>
- Cryptonet. (n.d.). *GRC - Governance, Risk Management, Compliance*. Retrieved from Cryptonet.it.
- Eshna. (n.d.). Retrieved from SimplyLearn.com: <https://www.simplylearn.com/financial-risk-and-types-rar131-article>
- Eurocontrol.int. (n.d.). Retrieved from <http://www.eurocontrol.int/articles/just-culture>

- Evans, D. (2015, 10 07). What is BYOD and why is it important? *Techradar.com* .
- Gleeson, B. (n.d.). Retrieved from Forbes.com: <https://www.forbes.com/sites/brentgleeson/2013/10/02/the-silo-mentality-how-to-break-down-the-barriers/#4a3817d8c7e9>
- Kapoor, G. (n.d.). Chief Operating Officer, MetricStream. *Governance, Risk Management, and Compliance: Creating the Right GRC Strategy for Your Company*. ExecBlueprints.
- KPMG. (n.d.). L'Enterprise Risk Management in Italia.
- OCEG. (n.d.). Retrieved from <https://www.oceg.org/about/what-is-grc/>
- Paolinelli, P. (2010, 01 22). *Trasporto aereo. Imparare dagli errori. Ecco cos'è la Just Culture*. Retrieved from paolopaolinelli.wordpress.com: <https://patriziopaolinelli.wordpress.com/2010/01/22/trasporto-aereo-imparare-dagli-errori-ecco-cose-la-just-culture/>
- Protoviti. (2009). Key Questions Regarding Integrated GRC.
- Quadrants, R. (n.d.). Retrieved from erm360.com: <https://www.erm360.com/tag/risk-quadrants/>
- Ramin Edmond, N. W. (2015, 11 11). Business move beyond the BYOD model. *TechTarget.com* .
- Reply. (n.d.). *G.R.C. - GOVERNANCE, RISK & COMPLIANCE* . Retrieved from Reply.com: <http://www.reply.com/it/topics/security/g-r-c-governance-risk-compliance>
- Richard Hunt, T. C. (2014, 06). Why governance, risk and compliance projects fail and how to prevent it. *Computer Fraud & Security* .
- Robert E. Hoyt, A. P. (2013). The determinants of Enterprise Risk Management: evidence from the appointment of chief risk officers. In *Risk Management and Insurance Review* (Vol. 6, pp. 37-52).
- Robert E. Hoyt, A. P. (2011). The value of enterprise risk management. In *The Journal of Risk Insurance* (Vol. 78, pp. 795-822).
- Seufert, N. R.-E.-A. (n.d.). A frame of reference for research of integrated Governance, Risk and Compliance (GRC).
- Skybrary.aero. (n.d.). Retrieved from http://www.skybrary.aero/index.php/Just_Culture
- Switzer, C. S. (n.d.). Co-Founder and President, OCEG. *Governance, Risk Management, and Compliance: Creating the Right GRC Strategy for Your Company*. ExeBlueprints.

- Victor Lipman, C. (2016, 06 01). Key Management Trends for 2016? Here are 6 Research-Based Predictions. *Forbes* .
- Vliet, V. v. (2015, 02 17). 3C model (Ohmae).
- Watson, Z. (n.d.). Why the market moved from Mobile Device Management to Enterprise Mobility Management. *TechnologyAdvice.com* .

APPENDIX

Figure 12: An example of the phases that a company should go through in order to reach the maturity level, called “Advanced GRC”

(Source: OCEG Illustrated;
<https://www.rsa.com/content/dam/rsa/PDF/2016/06/tool-ocog-pictographic-journey-to-advanced-grc.pdf>)

(image on the next page)

The Journey to Advantaged GRC

As organizations mature their approach to GRC, they transition from a structure of siloed departments and units to a fully engaged business operation where everyone has a part in managing risk, ensuring compliance and contributing to performance outcomes. This leads to greater confidence, agility and resilience - advantages that ensure success.

DEVELOPED BY


 The Security Division of EMC

Siloed GRC

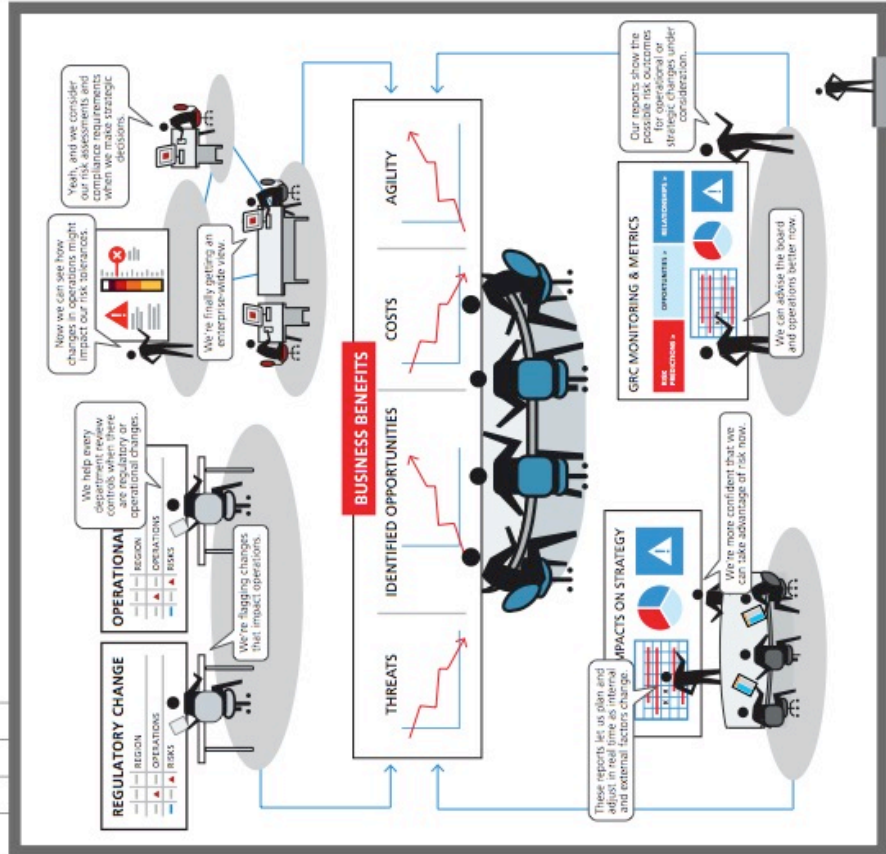
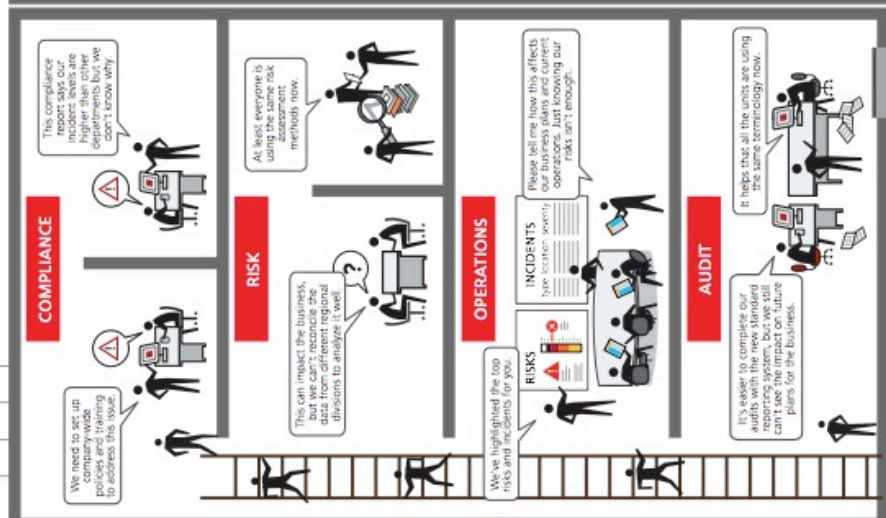
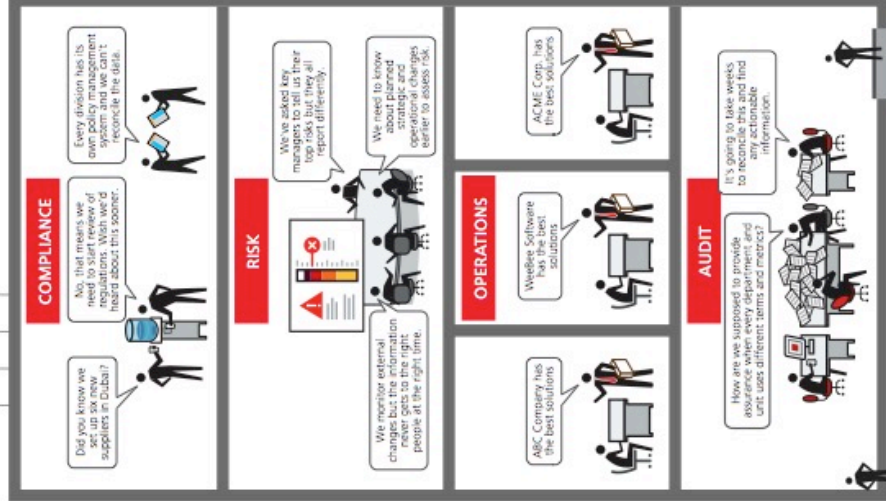
- Focus on compliance
- Reporting is disconnected
- Processes are isolated

Managed GRC

- Focus is on risk
- Reporting is coordinated
- Processes are defined

Advantaged GRC

- Focus is on business opportunity
- Reporting is enterprise-wide
- Processes are optimized



TRANSITIONING
 focusing on repeatable processes

TRANSFORMING
 focusing on business operations