Compliance Excellence in the Insurance Industry
Contents

Management summary

What Compliance in Insurance is about – scope and perimeter of compliance management

Pillars of an efficient and comprehensive operating model

- Organization

- Processes and methodologies

- Technology

Closing remarks

Appendices

Contacts
Management summary

Despite its youth compared to similar functions in the Banking industry, Compliance for insurance is yet a key player that makes the Board in control while infusing risk culture throughout the organization. Increasing regulations, internal and external environment complexity, and stronger client awareness are putting pressure on CCOs to capture incoming risks therefore increasing their span of control over the company-impacted processes and relative controls in place.

In this research, we collaborated with the top 15 insurance players at global level by GWP and market capitalization, to assess their relative position toward both the average of the industry and the benchmark, assumed as the excellence across all the areas of investigation. To do that, we structured a 150-question global survey across several dimensions of Compliance operating model. Each company is receiving feedback of this survey with its specific results. In this document, the readers will look at consolidated results.

Our survey reveals that the correlation between increasing regulations and cost of compliance is still positive with a further increasing patterns. Key drivers of such a trend are:

- **Un-lean organization.** With increasing risks and regulations, relatively far from the comfort zone of current CCOs and Compliance Teams’ talent profile and background, the organizational shaping of the Compliance Function has become a strategic choice that must be driven by a conscious and well-balanced approach across four key dimensions: roles & responsibilities in terms of CCO profile, purpose of the unit and key interactions on top of those that are mandatory; clear reporting lines going beyond dotted-line for reporting to the Board and a more efficient internal organization; a re-calibration between centralization and de-centralization in both horizontal and vertical directions to be more nimble; a fine-tuning of the span of control in terms of risks managed and activities performed

- **Flat processes.** The effects coming from the industry forces (customers, technologies, shareholders and regulators) put pressure on CCOs who are constantly requested to increase the span of control on their activities but, on the other side, are not allowed to properly increase their staff due to budget constraints. In such a competitive environment, CCOs must necessarily gear up themselves to review their methodological approach in order to increase the effectiveness and efficiency of the activities under their control. A three-step approach (“Excellence in core processes”, “Shift from risk mitigation to risk prevention” and “Compliance culture infusion across the Company”) is what we see as a roadmap for radicalization of compliance management into business processes, without increasing the burden of costs on the function itself

- **Dis-integrated architectures with limited scalability and unexploited potential of innovation.** At present stage CCOs should go beyond improvement of underlying architecture and applications (that remains a must). They should leverage on innovation to support the journey toward the “collaborative” model. We see major opportunities for Companies to leverage on RPA (Robotized Process Automation) and Cognitive computing to effectively capture risks and control processes while keeping the cost of compliance under control: such solutions can release early efficiencies, thus allowing for a quicker achievement of benefits with respect to multi-year big data & analytics journeys.

The key challenge is clearly “how to remain effective as a function limiting the cost of compliance increase”. The answer in our view is pretty mixed and it passes through:

- The adoption of a risk-based approach to manage the variable perimeter of laws and regulations that might significantly influence the non-compliance risk events

- A fundamental review of the target operating model across organization, processes and technology, evolving toward what we call the “collaborative compliance”, addressing the opposite needs of lowering costs while keeping the company in control

- An investment in technology innovation with main regard to Robotics and Cognitive computing to enable faster transformation, as well as Big data & analytics for midterm benefits

---

1 Consistently with this, Accenture 2016 Compliance Risk Study also came to the conclusion that Compliance will need to leverage other functions (e.g. Chief Data Officer) in order to deliver on more complex responsibilities whilst managing costs.
What Compliance in Insurance is about – scope and perimeter of compliance management

In the latest years the role and scope of Compliance in the Insurance market has been rapidly reshaped, notwithstanding its relatively recent application to the industry\(^2\). While the typical job of compliance officers used to be predominantly a “check the box” mixed to policy issuing, it now involves the setup and verification of the practical application of the control environment through numerous reviews against a broader set of laws and regulations.

Compliance, under a modern perspective of its role as a proactive means of prudential surveillance aimed to prevent, localize and minimize non-compliance and reputational risks, is called to continuously monitor a number of laws, regulations, regulatory requirements and internal policies. Therefore, one of the key questions is: what kind of regulations should fall into the control of the Compliance Function, without generating redundancies or affecting performance control?

The answer is not easy and unique, as the perimeter of laws and regulations under the responsibility of the function looks extremely diverse across the industry, between various countries, business segments or federal/state level, but the trend is that of a progressive expansion of such perimeter not only to sources legally binding, but also to the broader principles of integrity and correctness (e.g. Basel II Committee indications for the banking industry). Such a dilatation trend of the compliance’s scope would risk to affect the effectiveness of the function itself. It is therefore advisable that some key principles are defined to limit the area of influence of the function.

As a general rule, we could say that the Compliance Function should set up internal processes/policies to ensure compliance to laws and regulations, keeping a specific focus on transparency, correctness of behaviors toward the customers, contractual information and contracts execution (taking into consideration the dimension and peculiarities of the company). Starting from this principle, it is then possible to deep-dive specific topics (e.g. AML) depending on their relevance for the industry. In an attempt to rationalize scope of the function, we can thus distinguish between:

- Laws, regulations strictly in the scope of the compliance function
- Laws and regulations impacting functions outside of Compliance direct span of control, but for which Compliance is a stakeholder in an advisory capacity.

Moreover, key principle through which ring-fence the area of influence of the compliance functions are:

- proportionality in respect of nature of the activity, size and complexity: despite its self-explanatory description, such a principle remains key in order to keep the function as effective as possible in comparison to the number of laws and regulations arising at a very high speed in the industry
- Nature and amount of the penalties (risk based approach): “the more the penalty, the more the risk” or vice-versa. Such a principle allows a calibration of the compliance intensity depending on the consequences of the non-compliance events
- consistency with the targets of the regulatory activities which to comply with: such a principle allows to focus on risks/events that might affect the technical and financial health of the companies reducing the appeal and reputation across the customers
- existence of specific control areas (e.g. Tax, Accounting), against which the compliance role could be lower

According to the above mentioned principles and on the results of our international survey, the key focus of Compliance Functions should be:

- Authority regulations
- AML – Anti Money Laundering, with higher focus on payment flows
- Anti-Bribery and Corruption
- Data Security and Data Privacy
- Complaints and Claims Management
- Fraud Management

\(^2\) Consistently with this, Accenture 2014 Compliance Risk Study also highlighted the relative youth of the function with the respect to the other industries ones
• Distribution and selling practices
• Conflict of interests
• Anti-Trust
• Transparency of contracts
• Taxation on premiums

On top of these laws and regulations, best practices suggest including:

• Company internal regulations, in particular those referring to previously mentioned laws with the aim to reinforce control on deviations
• Qualification and/or framework contracts of providers and outsourcers of selected company functions, including compliance
• Ethical codes
• Agreements with customers’ associations
• Promotions and advertising
• Quality certification

Customer centricity is therefore one of the key focus of Regulators, as an increasing number of requirements are impacting Insurance core processes such as Underwriting, Product Development and Distribution.

Looking forward, some of the most impacting Regulations expected for the next years are:

• PRIIPs - Packaged retail and insurance-based investment products - effective from 1/1/2018, that requires companies to produce a key information document (KID – a simple document giving key facts to investors in a clear and understandable manner) covering not only collective investment schemes but also other ‘packaged’ investment products offered

• MLD4 – Money Laundering Directive 4 – Effective from 2017, updating the requirements in terms of Anti Money Laundering and Anti-Terrorism Financing
• MiFID II, effective January 2018, accelerating on full disclosure to customers of product features
• IFRS4, effective January 2018, focusing on balance sheet rules and reporting requirements
• IDD - Insurance Distribution Directive – effective from 23 February 2018, that regulates the activities of insurance intermediaries, insurance companies, their employees, ancillary insurance intermediaries as well as online distribution about the information that should be given to consumers before they sign an insurance contract
• GDPR - General Data Protection Regulation – Effective from 25 May 2018, that extends current data protection laws to all foreign companies processing data of EU resident and provides an harmonization of the data protection regulations throughout the EU
• HLA - Higher loss absorbency requirements – Effective from 2019, capital requirements that apply to the identified Global Systemically Important Insurers (G-SIs)
• ComFrame – Common Framework for the Supervision of Internationally Active Insurance Groups – Effective from 2020, requirements focusing on the effective group wide supervision of internationally active insurance groups

In this scenario it is clear that, more than the severity of sanctions, the risk to incur in reputational problems with the market is an additional issue for CCOs that gives the Compliance Function a strategic role within the Companies.
Pillars of an efficient and comprehensive operating model

The insurance market is experiencing an important transformation phase driven by the evolution of its key forces and players:

- **Customers**: seeking for products with new features and innovative services, potentially bundled and/or scalable
- **Technology**: reshaping business model but exposing the company to new risks (e.g. cyber threats, data protection, frauds)
- **Shareholders**: looking for relatively low risk investments with high & stable returns protecting their capital
- **Regulators**: strengthening and increasing the overall control on the industry

The joint effect of these factors is an increasing complexity of the ecosystem, putting pressure on Chief Compliance Officers (CCOs) who are constantly requested to increase the span on their activities (over the past 5 years the cost of risks and compliance has significantly accelerated) but, on the other side, are not always allowed to properly increase their staff due to budget constraints.

Therefore if the CCOs had the chance to rethink their compliance model from scratch, we believe they would ask for a disciplined, effective and efficient one along the organization, the processes and the IT:

- Disciplined, implying a consistent alignment and collaboration with other governance units
- Effective, reinforcing the power of risk mitigation actions and processes, covering a broader range of risks (including those emerging through the digital revolution) and improving its span of control
- Efficient, leveraging on the right mix among talent, models and technology, keeping the cost of compliance within reasonable boundaries, avoiding redundancies across functions and promoting clear lines of accountability in performing risk control

Organization

Attributes and dimension of the Compliance Function for Insurers

The organizational shaping of the Compliance Function is such a strategic choice that must be driven by a conscious and well-balanced approach. The journey that brings companies to define their organization blueprint is undoubtedly mind bending and we believe it should take into account at least four relevant dimensions:

1. Role and responsibilities in terms of CCO profile, scope of the function and interactions
2. Organizational model options (structure of organization charts and hierarchical/functional governance)
3. Activities balance footprint (centralization degree and areas of expertise)
4. Span of control (type of risks managed and activities performed)

![Figure 1. Compliance management organization – Key dimensions](image)

3 See also Accenture 2016 Compliance Risk Study.
4 According to Accenture’s “FY15 The Future of Compliance” study, 44% of Companies are looking for cost reduction initiatives for the next 1-5 years.
1. Role and responsibilities

Compliance scope

Regulators offer relative freedom to Companies on how to structure their Compliance Function: this is driven by “proportionality principle” to combine relevance of controls with size, structure and characteristics of the Companies’ market. Therefore Compliance scope can be variable in its shape.

In our view, the scope of the Compliance consists in focusing on the prevention of administrative penalties and the avoidance of potential assets / reputational losses connected to law violations or internal regulation violations. Moreover, Compliance should keep high focus on transparency, correctness of behaviors toward the customers, contractual information, contracts execution and customer protection as well as on the proactive training on regulations and compliance matter for the employees.

Most of Companies have already established a dedicated Compliance Function within their organizations. They appointed a Chief Compliance Officer to manage it (~90% of the interviewed panel) recognizing its relevance by distinguishing its activities from those under the responsibility of the more mature areas such as Risk management, Legal Dept. or Internal Audit. This did not happen by chance, but because Compliance requires by itself an adequate level of autonomy for evaluating appropriately the potential risk of misalignments between the Companies Operating Models and the regulations impacting them.

"Most of Companies appointed a Chief Compliance Officer (~90% of the interviewed panel) recognizing its relevance by distinguishing its activities from those under the responsibility of the Risk management, Legal Dept. or Internal Audit areas."

Figure 2. Profile of the Chief Compliance Officer

Solvency II & EU Directive 2009/138
- Prerequisites
  - Honoreability
  - Competence
  - Professional qualification
  - Reputation

Proportionality and principle-based approach
- Role profile
  - Dedicated role
  - Independent from operating units
  - Potentially an administrator
  - Direct functional and hierarchical report to BoD

Best practice
- Core responsibilities
  - Direct responsibility of compliance activities, independently from organizational structure
  - In charge of direct communication to BoD

Market context
- Extended skill-set on top of traditional
  - Business knowledge
  - Big Data & Analytics
  - Cyber and digital risks
  - Robotics capabilities
CCO and Compliance Officers talent profile

To handle Compliance Management activities and given the rising regulatory pressure impacting the industry (in particular Solvency II and EU Directive 2009/138), particular attention must be paid to the choice of the Chief Compliance Officer who is asked to match strict prerequisites in terms of honorability, reputation, competence and professional qualification. As a matter of fact, having placed Compliance into the Internal Control System (ICS) area implied to define how the CCO plays within the key reporting lines (both hierarchically and functionally), since he/she should neither be appointed as head of an operating unit, nor as depending on those areas. Such a dilemma is solved by placing the CCO within a BoD reporting line, ring fencing in his/her hands the responsibility and the coordination of people involved in controls, independently from the organizational model.

Moving to compliance professionals skill-set, since few years ago the profile of the resources that were most valued for Compliance Management area were the ones presenting strong legal and risk management skills.

By contrast, nowadays Technical Business skills are chased because best practices show that Compliance risks are better detectable when the analysts can unveil all the possible consequences behind a certain process or a certain organization which they are keen on. The more the Compliance unit can get to the heart of the business matter, the more effective are the controls carried out, in terms of both prevention and detection. As a consequence, HR and Organization play a fundamental role in managing internal turnover of people involved into compliance or compliance-related activities, and talent pools for recruitment are now more diverse (e.g. banks are looking to military for surveillance skills) in order to guarantee to the Compliance Function the most effective mix of talents.

Business functions engagement

As mentioned, to get to the heart of the business, the Compliance area needs business skills and strong business engagement. It is a tried-and-tested evidence that risks should be detected and addresses directly where they are run in order to be promptly mitigated. Business competences help the Compliance unit to smooth the relationship with Business Operating Functions and the overall risks assessment activities.

Basing on our experience, a viable accelerator to reach this cooperation between Compliance area and Business Operating Functions, as well as the Business skills infusion in Compliance area, could be the adoption of a job rotating approach that allows to reinforce Compliance unit receiving some skilled resources coming from other operating functions.

Compliance unit independence

Regulators generally require that the structure and the degree of coverage of the Compliance Model adopted should be proportionally adequate to the Company overall complexity (size, type of business, geographical fragmentation, etc.). Therefore there is no “secret source” in setting up the right Compliance model, but a continuous improvement process that follows the Company evolution is what that the regulations really imply.

Independently from the model adopted, the Compliance area should always respond directly to the Board of Directors in order to:

- preserve itself from the Operating Business Functions influences
- guarantee maximum access to information
- allow a direct relation with the Board when exposing the results on the overall compliance status

“The Compliance unit needs business skills and strong business engagement to be effective. The closer it can get to the heart of the business, the more effective are the controls it carries out in terms of both detection and prevention."
Compliance unit independence is a key aspect to preserve the quality of the Compliance Management results. To protect its impartiality, Companies decide usually to put in place several rock-solid actions like for instance to maintain the control of the Local Compliance budget under the responsibility of the Group Compliance (and not under the control of the Legal Entity governance), or for example to build ad hoc remuneration / incentive models for the Local Compliance resources.

**Compliance unit within the Internal Control System**

The Compliance Management takes part to the overall Internal Control System of the Companies and plays an active role coordinating its activities in particular together with the Risk Management (2nd line) and Internal Audit (3rd line) (see the “Three-level defense model” – Figure 3).

**Figure 3. Three-level defense model**

Establishing a “front to back” view of risk across the three lines of defense, starting with the front line, is a fundamental challenge for the Internal Control System and the Compliance function itself.

To avoid inefficiencies and misalignments in the overall model, it is strongly relevant to distinguish the different roles played by the various Internal Control System functions:

- **Compliance Management**

  The Compliance Function acts as a second line of defense providing the first line of defense (handled mainly by Operating Business Functions) with all relevant methodologies, tools and evidences on regulatory requirements impacting the business activities, as well as training and subsequent compliance monitoring.

  Once performed the risk assessment, the Compliance Function supports the business in determining the remediation actions to put in place for the detected areas of risks and monitors the overall risks indicators in order to provide an overall overview to the Board of Directors.

  Under this perspective, Compliance assures the consistency of the business conduct of the company toward regulations (external and internal) to prevent non-compliance risk, expressed as the Risk of penalties (by law or administrative), losses or reputational damages due to inobservance of laws, regulations of Authorities, internal rules and policies.

Such a control activity should be systematic, recurring, prudential and proactive (e.g. forward-looking analysis of laws and regulations). One of the key of the nature of the activity is that the Function is asked to spread across the company a culture of compliance (e.g. Solvency II directive explicitly states that selected risks can be managed by governance requirements instead of quantitative solvency requirement)
### Risk Management

Risk Management (which may consist of multiple functions, e.g. Liquidity Risk, Credit Risk, Operational Risk, etc.) acts as a second line of defense too, it evaluates the risks at which the Company is exposed within an acceptable level, considering company available resources. Even though methodologies and analysis approach could be similar between the compliance management and risk management and some overlaps could be identified, it is important to remember that the final scopes of the two entities are different. Risk Management is focused on determining quantitative metrics for identifying the risk capital requirements. On the opposite the Compliance Management is focused on identifying area of non-compliance to regulatory and remediation plans.

### Internal Audit

The Internal Audit acts as a third line of defense monitoring, assessing and maximizing the effectiveness and the efficiency of the Internal Control System.

It performs assurance and advisories activity to the company functions, supporting them in their alignment needs ad identifying further areas of intervention.

### Legal

The Legal area provides valuable opinions on current or upcoming laws in order to let the different lines of defense be ready to evaluate the operating model in place and its adequacy with regard to regulations. Its advice is strongly useful since regulations can be valued and interpreted very differently on the base of the diverse practices.

---

#### Figure 4. The Compliance Function within the Internal Control System

<table>
<thead>
<tr>
<th>Topic</th>
<th>Risk Management</th>
<th>Compliance</th>
<th>Internal Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Priority focus</strong></td>
<td>• Keep risks at which the Company is exposed, within an acceptable level, considering company available resources</td>
<td>• Ensure compliance to laws, reg. requirements and internal proc., avoiding non-compliance risk (page 3)</td>
<td>• Monitor, assess and maximize effectiveness and efficiency of the internal Control System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Keep high focus on transparency, correctness of behaviors towards the customer, contractual information, contracts execution and customer protection</td>
<td>• Perform assurance and advisory activity to different company functions, supporting them in their alignment needs</td>
</tr>
<tr>
<td>Core skills &amp; competencies</td>
<td>• Risk modeling and evaluation</td>
<td>• Knowledge of laws, regulations and procedures and their impacts on company processes</td>
<td>• Knowledge of rules and operational practices</td>
</tr>
</tbody>
</table>
| Responsibilities       | • Identification, assessment and control of most significant/material risks affecting company solvency or realization of objectives | • Assessment of non-compliance  
• Proposition of mitigation actions | • Verification of effectiveness and efficiency to increase risk management processes  
• Verification of processes effectiveness and efficiency in order to identify improvement areas |
2. Organization model options

**Organization structures**

Organization models currently in place could differ significantly on the base of several influencing factors such as company’s overall blueprint, complexity, size, geographical coverage, business domains and growth history (i.e. acquisitions, integrations, etc.).

On the base of our study, three most relevant organization models have been detected:

- **“CRO staff” model**

  (Compliance unit reports to the CRO and it is managed together with Risk Management).

  This model allows to leverage on synergies coming from common methodologies that both Compliance and Risk management adopt and to leverage on an overall skills set enlargement for Risk and Compliance Management resources.

  Nevertheless, this model could bring some inefficiencies due to both potential conflicts in pursuing the respective objectives that are different between Compliance and Risk Management and due to the not direct relationship between Compliance Management and the CEO/ Board of Directors.
• “General Counsel staff” model

(Compliance unit reports to the General Counsel and it is managed together with Legal).

This framework avoid activities duplication regarding regulations and laws interpretation thanks to the closeness of Legal and Compliance resources. Strong legal competencies characterize the Compliance resources operating in this context, as per the common practice in the market.

On the contrary it typically implies poor business skills and limits on the exposure of Compliance area to business functions with consequent ineffectiveness of the control activities.

• “Stand alone” model

(Compliance unit reports directly to CEO and Board of Directors).

This model guarantees focus on key control processes, consistency with the increasing complexity of Compliance overall environment and strong independence from the other functions. Being more structured, in this context Compliance unit could be more expensive in terms of resources and other costs absorbed if not managed within a well-balanced framework.

**Recommended option**

Compliance unit positioning within the overall Company organization chart highly influences its degree of autonomy and independence that must be preserved and protected as explained in previous chapter.

For this reason the Compliance dedicated stand-alone function is the most suitable to address increasing complexity of market environments guaranteeing at the same time strong independence and direct access to Company information thanks to the relationship with the Board of Directors and the participation to Business Committees.

**“Stand alone model with a direct reporting line to BoD (currently adopted by only 23% of the market) is the most effective option to guarantee independence and direct access to company information.”**

---

**Figure 5. Main organizational structure options**

<table>
<thead>
<tr>
<th>Reporting line</th>
<th>Strengths</th>
<th>Weaknesses</th>
<th>Frequency</th>
</tr>
</thead>
</table>
| CEO staff      | - Skill-set enlargement, in particular within the internal control system  
|                | - Possibility to exploit synergies of control specifically regarding the operating risks | - Limited independency from other functions  
|                | - Synergies with legal department (resources)  
|                | - Sharing of core skills/competencies | - Possible clash within the 2nd line of defense due to controls allocation |
| G. Counsel staff | - Focus on key control processes  
|                | - Consistency with regard to the growing market complexity and (in some Countries) to the regulators requirements  
|                | - Strong independency | - Complexity in integrating similar competencies (SCI) and business ones  
|                | | - Limited exposure to business and processes topics |
| Stand-alone    | | - Higher costs (staff and other administrative expenses)  
|                | | - Overlapping risk with regard to other function scoping area |

---

11
3. Activities balance footprint

Activities balance footprint is the third key dimension through which to shape the Compliance Management, basing on two strategic questions that should be addressed:

- how to organize activities within the Function
- how to centralize/decentralize the activities along the “horizontal” and “vertical” axes

Compliance unit activities organization: addressing the cost of specialization

According with market evidences, Compliance unit can be structured by risk type, by processes or through a blended solution (by line of business):

- **Organization by risk type**
  
  Organizations structured by type of risk (43% of our survey) have dedicated Compliance sub-units per type of risk and a single compliance point of contact for internal and external referents (i.e., regulators). These solutions allow to set up a major risk specialization (suitable especially for some risk clusters such as AML, and Data protection), a clear interface for regulators and easier integration for emerging risk (e.g., Cyber, Terrorism). On the contrary, they imply poor operational efficiency due to limited synergies between cross-risks common processes (mainly reporting) and relatively higher resources absorption on selected activities.

- **Organization by process**

  Organizations structured by process (7% of our survey) specialize resources by area of activities (e.g., Risk Assessment, Reporting). Under this approach a maximum exploitation of synergies is guaranteed thanks to the standardization of the activities and thanks to their “cross-risk type” industrialization.

  This approach on the other hand offers poor specialization on specific risk matters and a consequent risk of underestimation of non-compliance risk effect on some key processes.

- **Organization by line of business**

  A sustainable alternative to organize Compliance consist in adopting a blended solution in order to adapt it to the specific needs of the lines of business. A mixed solution (by risk and process type; 29% of our survey) can in fact combine risk specialization for main complex (e.g., AML) or emerging risks (e.g., Cyber risk) and a standardization of common processes for the remaining areas of risk, guaranteeing operational efficiency according to the lines of business needs.

---

![Figure 6. Compliance unit internal organization models](image)
Compliance unit activities centralization/decentralization: finding the right “Horizontal” and “Vertical” balance

While designing the organization of the Compliance function it is necessary to clearly define the different responsibilities in charge to the central and local offices (vertical centralization/decentralization) as well as the activities directly performed by Compliance unit itself and the ones delegated to other Business Operating Functions (horizontal centralization/decentralization).

The choices taken by Companies on these aspects are often driven by their characteristics in terms of business complexity, size, legal environment, thus influencing many additional factors such as the staffing of Compliance Unit and the skills required. Notwithstanding that, we see two prerequisites to be in any case guaranteed:

- When delegating to other Business functions part of the Compliance activities execution (i.e. risk assessment, monitoring …), Local Compliance Officers should be always accountable for them, even if they are performed externally.

- Local Compliance units should always have a direct functional reporting line with Group Compliance structure in order to limit local Business functions influence and constrains on compliance controls execution.

We detected four main behaviors that usually correspond to specific characteristics of the Companies (Figure 7):

- Horizontally centralized model
- Horizontally decentralized model
- Vertically centralized model
- Vertically decentralized model

See also “Teoria e prassi della compliance nelle assicurazioni”, E. Casarin

---

5 See also “Teoria e prassi della compliance nelle assicurazioni”, E. Casarin
Even though there are multiple combinations of vertical and horizontal dimensions, we could say that:

- **Local Compliance** should at least:
  - keep monitored the local regulatory landscape in order to detect possible impacts on Company structure (local and global)
  - produce the adequate reporting to the governance
  - support the Business Operating Functions in handling the risk assessments to identify potential compliance breaches (providing standards and methodological support defined at global level)

- **Group Compliance** should at least:
  - prepare the internal regulations and policies
  - define methodologies, frameworks and a group-wide risk taxonomy
  - manage an high level global regulatory observatory coordinating the local ones
  - coordinate local compliance activities with higher focus on risk assessment and risk reporting

**Recommended option**

In a context of increasing complexity and fast moving scope of the compliance area of influence, Companies should moderate their compliance shape toward a “vertically” and “horizontally” decentralized model for selected processes, acting as a Competence Center and allowing:

- strong integration with the business functions hold responsible for the key controls
- higher effectiveness of execution
- higher efficiency and greater business engagement

Furthermore, in terms of organization of activities within the Compliance area, a blended model combining strengths of “by risk type and by process type models” is the recommended one. In this way high level of automation for cross-risk processes as well as strong specialization for complex risks could be pursued thanks to an accurate shaping of activities organization.
4. Span of control

Activities and risks managed

Each Company should tailor the scope managed by its Compliance unit on the base of size, complexity and non-compliance risk associated. Choices in term of perimeter of activities are key in order to influence the effectiveness of the controls performed. Processes covered and risks audited are the two relevant dimensions that qualify the nature of the Compliance unit within the Company.

In such a complex environment, Companies should tend to not limit their span of control to core Compliance processes and relative risks (focusing on controlling ex-post the existing basic potential non-compliance areas), but to extend the scope of their activity including the anticipation of increasingly complex and prospective risks (what we call “Extended compliance”), embedding ex-ante controls and evaluation, forthcoming new regulations analysis and new technological trends detection.

Finally, as a step of further enhancement of its role within the organization, Compliance should pay more attention to the infusion of Compliance culture at 360° degree in the firm through a set of initiatives that helps to sharpen employees acumen on Compliance matters (what we call “Collaborative compliance”) such as training, incentive initiatives, integration with business activities (e.g. products development, underwriting, pricing, etc).

Figure 9. A possible vertical and horizontal centralization balance (illustrative)
Most advanced Companies extend in fact the area of influence of the Compliance also to the other Business Functions business-as-usual activities. This is managed through the inclusion of the Compliance into the most relevant decision nodes (e.g. participation to Company’s Committees).

On the basis of the adopted model for what it regard the activities span of control, the level of centralization and the internal organization of the function, Compliance should have an adequate staffing that implies to guarantee an allocation of an appropriate number of resources with specific skills that allow to handle efficiently and with efficacy compliance unit activities.

“Pioneer Companies are preparing themselves to the forthcoming regulation complexity increase moving toward a collaborative Compliance model capable of proactive prevention and 360° compliance culture spread within the firm.”
Sizing and skills

There’s no “one size fits all” solution to identify the appropriated magnitude of the compliance function to be put in place. In particular there’s no direct link with a specific parameter of the company (such as the overall business volume) that determines how structured the Compliance unit should be.

On the opposite, more often the size of the Compliance unit (both at Head Office and at Local level) is the fruit of a complex mix of several factors that make unique the framework of each individual firm.

This explains also why players that seem apparently similar (in terms of business volumes and business models) often have completely different sizing for what it regard their Compliance function.

For instance, our analysis highlighted that there’s no direct link between the business volume (i.e. Gross Written Premiums) and the number of FTEs allocated in the Compliance function as intuitively several people could think (see Figure 11).

On the contrary, the main rationales to be investigated when determining the size of the Compliance function are:

- the set of processes covered by Compliance function
- the level of interaction that the Compliance has with the other functions
- the complexity of the offering (e.g. # of products offered by the company, …)
- the type of business (e.g. direct, bancassurance, traditional, …). With the growing of the complexity to be managed in terms interactions (with risk management, internal audit, supervisory authorities and other organization functions), processes covered, company business model blueprint and geo’s footprint, the request of resources to be allocated to the Compliance function inevitably rises.

Figure 11. Compliance unit sizing and Company dimension – Market watch

Figure 12. Compliance unit sizing vs. other factors – Market watch
Generally speaking, on the base of our study we detected that the size of the Compliance function varies on average within these ranges:

- for Local and BUs Compliance units: 5 – 30 FTE
- for Group Compliance unit: 10 – 35 FTE

These ranges must be used carefully and must be taken as illustrative references because often there are other additional factors influencing the overall sizing of the compliance unit that are not controllable/addressable. Between them we can mention for instance:

- the M&A journeys that the Companies could have undertaken in the recent past (in fact inorganic growth often is not followed by an effective integration of the former operating units, creating duplication of activities and missed synergy opportunities)
- the usage of some Shared Service in order to run some standard activities in outsourcing

As mentioned before we are assisting to a shift in the professional’s skill-set chased for the Compliance area. Additionally to the strong legal and risk management skills, nowadays Technical Business skills are required as well in order to detect the possible consequences and risks behind a certain process or a certain organization.

Independently from the skill set required, what it rises from our study is that the industry lacks fresh outlook and perspective but strenuous efforts are being taken to address this.

“Average size of Compliance function varies from 5 to 30 FTE for each Local and BUs Compliance unit and from 10 to 35 FTE for Group Compliance unit.”
Recommended option

Going back to the possible Compliance models to be adopted, we could say that the “Collaborative model” is the suggested one when the Company has the size and the resources to sustain it (size and resources must be evaluated on the basis of what explained in the chapter here before).

It guarantees strong integration and facilitates the Compliance “culture” expansion within the firm helping in anticipating/addressing the potential areas of non-compliance or in recovering the already existing compliance-breaches. Despite a major initial effort and resource absorption, it allows a non-proportional increase of resources, when new risks/new processes come under compliance area.

What is on the horizon?

Insurers are willing to deploy efficient organizational models with strong business involvement to avoid:

- duplication of activities
- extremely large numbers of controls without a risk based approach
- large departments carrying out manual tasks.

To address these goals the market is still evaluating additional possible solutions.

According to our study, these are some of the prospective options:

- set up centralized shared services (cross-insurance industry carriers) to leverage economies of scale/competence (sharing of resources with other insurance companies for the delivery of certain Compliance processes will be key to long term sustainability of Compliance operations)
- outsource the non-core activities
- activate robotics solutions to automate basic and recurring controls, reducing structural costs
Processes and methodology

On the process side, we recognize three main steps that delineate the possible “evolution” for compliance functions:

1. Excellence in core processes
2. Shift from risk mitigation to risk prevention
3. Compliance culture infusion across the Company

These steps are only conceptual phases that we consider viable in the path to the highest radicalization of compliance Management into business processes: for that reason they could be activated in parallel and not sequentially.

**Figure 14. Core processes under the Chief Compliance Officer’s responsibility**

1. **Excellence in core processes**

We consider as “Core Processes” those processes usually, and historically, under each Chief Compliance Officer’s responsibility:

- Regulatory Alignment
- Compliance Risk Assessment
- Reporting
- Advisor

**Regulatory Alignment**

Regulatory detection and new requirements interpretation represent the starting point for all Compliance activities: it could seem just a mere mechanic and repetitive exercise, but in fact it is not. It requires attention to details, competencies and strong judgmental capabilities to properly identify the connections with business peculiarities of each company. Such a process implies not only the detection, update and analysis of relevant rules and regulations, but also (and above all) the connection between those laws/rules and the company’s processes. Moreover, Regulatory alignment should be inspired by a forward-looking approach, aimed to get anticipated awareness of the potential effects of laws.

According to our survey results, some of the interviewed players revealed that they are using external provider services to timely identify new regulatory requirements. While we believe that the detection activities could strongly benefit of the use of external providers (and we encourage their use to our Clients), the interpretation of these requirements is a crucial activity to be performed jointly by Compliance and Legal department.

The outcome of this activity is the formalization of core requirements that must be defined in a simple and clear way: we suggest to avoid a rigid legal approach, using a user-friendly language to explain in easy terms the meaning of the requirements and the related level of sanctions.

In our view, excellence in Regulatory alignment means to excel in the activity of association of relevant laws and regulations with company’s processes (assuming full mapping and description of business processes provided by Organization Department): a key outcome of such an activity is the so called “law-to-process matrix” that combines the content of relevant laws and regulation with the processes at the single activity level, where each activity is mapped as
either a common one or a key control. Through such an approach, evolving perimeter and/or modification of existing perimeter are matched with the relevant controls and those controls can be consistently verified (or in case updated).

The key ingredients of the matrix are:

- A legal and business skill set
- An initial material effort for building the matrix itself
- The definition of rules to highlight changes and effects across the processes

With a higher focus on the third point, analytics and big-data drive technologies could favor the automation of the cross-process monitoring, leveraging on the adoption of clue words, smart semantical connections and infer from large volumes of information analysis complex relations with the aim to structure detection patterns.

Compliance Risk Assessment

Compliance Risk Assessment is the fundamental exercise run by Companies, aimed to measure the potential loss by non-compliance risk at single process node. Such a focalization sometimes causes not to tie the entire compliance picture together. Compliance Risk Assessment is typically structured into two phases:

- Evaluation of processes and controls
- Risk-Control-Assessment: self-assessment, by process, of key controls in place to prevent non-compliance risk

In the first phase, Compliance scans company’s value chain and processes to identify key areas at risk, assessing the inherent risk (defined as the risk embedded into the activity/process, not considering mitigating actions to offset the exposure). Such an exposure can be measured through different approaches:

- Frequency of the activity per non-compliance loss, often identified as either the average or maximum penalties for the case of non-compliance
- Historical approach, based on past-event data

Once inherent risk has been identified, Compliance evaluates key controls in place across the activity/process, calculating the “residual risk”, identified as the inherent risk net of key controls in place. To avoid excessive complexity, we suggest to simplify the approach in order to distill insights and provide clarity to the 15/20 most important compliance risks the company is exposed to, therefore enabling proper risk oversight by the Board and Top Management.
The central point of our suggested approach is to create a “key risk register” sharing it with all other risk heads outside Compliance, where all relevant information is stored in order to track properly the risk exposure. As a pre-requisite it is important to structure a simple and clear risk taxonomy with evidence of the main risk typologies identified by the company (Customer verification, suspect operations,...), the related Risk Categories (Penal, Administrative, ...) and Risk Impacts (High, Medium, Low). The register could also help drive efficiencies in other types of risk assessment (e.g. operational risk assessment).

Such an approach that we consider relatively easily applicable by CCOs, comprehends the following methodological steps:

- Identify, for each of the core requirement defined in the “Regulatory Alignment” phase, the related Risk Categories, Risk Typologies and Risk Impacts
- Detect the Value Chain areas and the key processes of the company impacted by those risk
- Determine the likelihood of each risk in terms of probability of occurrence basing on the already discussed methodologies
- Identify and assess mitigating factors in place (such as Training programs, policies, IT procedures, ...) 
- Identify and assess all controls/inspections in place (1st and 2nd level)
- Produce a structured non-compliance risk reporting, in the shape of a heat map, measuring both the current situation and the gap toward desired target picture

This approach provides several benefits to the company:

- provides results quickly allowing its application multiple times during the year
- enables CCOs to focus on key risks, avoiding duplication of effort with other units

Subsequently to the sharing with Top Management of key risk and priorities, Compliance could promptly move toward mitigation actions definition in order to reduce risk at an acceptable level.

In the next phase, not necessarily subsequent to the “Evaluation of processes and controls” phase, each unit is called to perform the risk-control-assessment, a bottom up review of the key controls in place, verifying effectiveness of design and operations, and ultimately to plan for mitigating actions in case of ineffectiveness of the controls themselves.

Compliance risk assessment allows to shape the heatmap of non-compliance risk for the entire Company, highlighting the core processes on which to concentrate about in order to address the gap.”
In our view, such a bottom-up approach facilitates the diffusion of a compliance culture throughout the organization and enables a model of extended compliance, reinforcing the accountability of the business functions. Involvement of business units or in general of units different from Compliance is key to adopt a preventive approach in the company.

Self-assessment is a key process that requires naturally major commitment of top and middle management, strong involvement of Compliance in addressing and coordinating the activities and as a prerequisite it needs a structured approach.

In our view, the bottom-up approaches should also not deviate from the proportionality principle and should therefore embed a risk-based logic, focusing on what should be done across the most relevant processes. In our study we verified that 86% of the companies surveyed are planning to sharpen involvement of business units into the process, covering also the incoming risks considered more relevant (data privacy and security, as per the 50% and 43% of the respondents respectively).

A sound approach of risk-control-assessment in a bottom-up perspective should be made of:

- a risk-based logic to focus on the most relevant risks; such a logic can be based on either the expected penalties in case of non-compliance or a de-composition of the balance sheet, locating the most frequent, company-relevant, regulatory-relevant processes (and related risks)

- a structured framework, in which the key processes are identified and mapped basing on the decomposition of the balance sheet, with details per single activity and per key controls in place (including ownership). To every process that crosses the entire company, a specific business owner is assigned as ultimate responsible, to guarantee compliance together with the CCO. Every process is then monitored and data are collected into a specific Compliance Cockpit, to enable CCOs and process owners to assess the compliance/non-compliance situation of the process itself and of the single activities and key control that compose the process.

Finally, mitigation is a key phase since it embeds the preparation and the execution of action plans to fill the compliance gaps identified across the Regulatory Alignment and the Risk-Control-Assessment. In this phase, the collaboration with Organization ranges from actions on people and organizational frameworks to processes and procedures. The key target is to further lower residual risk within the limit of the overall company’s risk appetite.
Reporting

If we ranked the less structured activities currently held by Chief Compliance Officer, reporting would probably be at the first place: from the findings of our survey, approximately 38% of the Clients interviewed revealed that their reporting processes are structured to some extent but with rooms for improvement, while the majority (62% of the panel) states that reporting is still “variable, non-automated and with large room for enhancement”.

Execute a good and detailed risk assessment process without properly structuring its reporting does not allow to effectively communicate the key messages to all internal and external stakeholders (mainly BoD, Top Management, Risk Owners, Control Owners, Regulators, Internal Audit).

Therefore, we strongly encourage investing in these areas through the identification of:

- structured reporting processes with internal and external stakeholders
- appropriate IT architecture and applications to adequately support the defined processes

Reporting is fundamental to:

- measure the effectiveness of the key controls in place: assuming the existence of the process-risk matrix and the attribution of the key processes to key control owners, a structured reporting framework enables to assess the effectiveness of the compliance activities (in terms of residual risk vs risk appetite) and efficiency, in terms of cost of the control compared to the non-compliance risk value, measured through the approaches analyzed before
- infuse the culture compliance across the organization, allowing control owners and business process owners to be aware of the risk they are managing or un-managing and the effects of their control activities in place (so called follow-up)
- prevent the rise of incremental risks due to prompt availability of metrics at process and activity level

Advisory

Compliance function, in addition to all the other duties mentioned above, provides advice on Compliance matters to several stakeholders on an ongoing basis.

This activity usually includes:

- Advisory to Senior management and Board of Directors to provide information about possible changes in regulation that could impact the company and the business decisions
- Advisory to business functions in the judgment of specific regulatory requirements or laws
- Assistance to business managers in formulating policies that comply with regulatory requirements

Under this heading might also fall liaison with regulators and other relevant bodies in respect of queries or enquiries about business priorities, issues and so on, or responding to consultation by providing the view of the company on proposed regulatory developments that could impact the Compliance environment.

Advisory represent an important part of CCO effort, with the complication that is always on demand, difficult to predict and with a strategical importance for the whole business: therefore, our main recommendation is to plan annual activities in an adequately way in order to save some spaces for the proper execution of advisory.

2. Shift from risk mitigation to risk prevention

Once core processes are secured, the second step in the compliance evolution toward excellence is to reinforce the focus on risk prevention rather than risk mitigation. In our view this is possible through an increased participation of CCOs in other company’s key processes.

Within this context, two areas to focus on are:

- Human Resources, with regard to “Education” and “Training” processes
- Insurance/Re-Insurance, with regard to “Product Development” and “New product approval” processes

Education and training

Complementary to advisory, training is one of the most relevant way in which CCO can spread compliance knowledge within the company.

Training could be a mean for an organization to demonstrate its commitment towards compliance and, at the same time, sensitize employees about the laws and regulations they must respect.

More specifically, training programs are one of the key ways for Compliance officers to inform the business about:

- compliance requirements and related sanctions
- possible consequences of not complying with internal procedure and processes
- importance of mitigation actions and system of controls put in place

An effective compliance training program should allow that potential risks are known and clearly identifiable by all resources, enabling the whole company to timely identify and address them with a forward-looking approach. From our point of view, there are some key principles to be followed in order to have in place an effective compliance program that are:

- provide training courses to all resources and check their knowledge through tests and certifications. These certifications should be maintained over the time in order to ensure that employees are kept up to date with changes and reminded regularly of their obligations.
training must be pitched at an appropriate level to properly engage resources: tailor the training according to the level of the employees and their duties within the organization (i.e. role-based training)

training material should be updated regularly

all the employees should be incentivized to attend a defined number of minimum hours of training (e.g. setting penalties in the annual performance evaluation process when the personal goal is not achieved)

training scenario should be tied to the real world (i.e. role playing, …), so employees can better understand the implications and consequences of their actions

Compliance training programs should use different channels/ media, not just traditional e-learning or classroom, but also new methods such as gamification, virtual reality, and “nudge” programs.

New Product Development and Approval

New product launch is one of the key strategic initiatives to strengthen market positioning, but presents a number of interconnected risks such as:

• Reputational risk
• Strategic risk
• Credit risk
• Compliance risk
• Other risks (liquidity risk, pricing risk, …)

Compliance contributions during product approval, mainly focused on Reputational and Compliance risk prevention, are multiple and could be summarized in the picture below, which represents an example of a standard product development process.

More specifically, Compliance role within the product approval process should ensure that:

• product features satisfy applicable regulations
• product literature is clear and not open to misinterpretation
• defined sales practices comply with applicable regulation

3. Compliance culture infusion

Creating a company-wide Risk & Compliance culture is a well-known as well as appealing theme in compliance discussions and it is presented as one of the key drivers for a real big transformation of companies.

An effective and positive compliance culture in place is an important protection against enforcement harm and collateral damage and can provide several benefits such as:

• increase the responsibility of resources in managing compliance risks
• have a better view and consciousness, at all level, of compliance risks at which the company is exposed

---

6 See also Accenture’s The Ethics and Conduct Challenge for US Banks: Learning from the UK Experience
better address the risks that arise in each strategic area
• increase the efficiency of processes and procedure and overall, optimize the cost of compliance
• enable more effective controls and ensure a better formalization of them for internal and external purposes
• reduce sanctions

Insurance players are trying to increase their resources perception of Compliance Management importance, but the goal seems still to be far: Compliance is often perceived as an “obstacle” instead of a business partner to support and increment the company success.

How is it possible to reverse this?

First of all with the proactive cooperation of all the resources working in the company, such as:
• Top Management - to promote the importance of Compliance culture and raise awareness of all 1st line resources in order to pro-actively cooperate on avoid compliance risk exposure
• Risk Management – for sharing the methodological approach and evaluate the possible losses related to operational risks
• Business Owners – for sharing, and not hiding, compliance and reputational implications related to business decisions and systematically adopting and monitoring key controls in place
• Process/ Control Owners – for respecting processes and procedures and promptly escalate emerging issues
• Legal – for supporting Compliance resources in the interpretation of regulations and laws
• Internal Audit – for sharing information about opened audit issues, planned inspections and controls in place

In addition to cooperation, we believe companies could leverage on other actions to further enhance the embedding of compliance culture within the company, and we would like to suggest two examples:
• Involvement of compliance function into hiring processes
• Establishment of compliance based incentive processes

Set up of compliance based incentive processes

In a world with no controls and incentives in place, many people would do the wrong things in many situations: starting from this assumption, we believe that incentives could be an effective tool to drive people toward compliance.

If you are still doubting about the effectiveness of incentives programs in promoting compliance culture, hereunder you can find the most clear and visible benefits of these initiatives. With proper incentives:
• People have an interest (an incentive) in respecting applicable regulations and avoid illegal conducts
• Management and Board can demonstrate a commitment to compliance themes and indicate the right path to be followed by resources
• Company is reducing its overall exposure to compliance risks

To further clarify our idea, we would like to present a couple of possible applications of these incentives:
• Resources performance evaluation
• Promotion requirements

In relation to the upgrading of the performance evaluation processes presented above, company could also set a minimum score on compliance related evaluation areas that should be met in order to become eligible for promotion.

Social studies reveal that the bigger the incentive is, the stronger is the effort of people for achieving the goal: this understanding could lead, on the other side, to the conclusion that misaligned incentive systems can encourage unethical or illegal conduct.

If people with a “compliance and ethic” attitude are rewarded and recognized for their behavior, they immediately become the models for succeeding within this organization: in this way compliance culture will be spread easily and at a relative cost providing an enormous benefit to the whole organization.

Involvement of Compliance function into hiring processes

The success in preemting and managing risks could also depend on the hiring decisions: hiring key candidates with a clear understanding of the importance of Compliance Management topics could diminish future risk exposure and facilitate the embedding of compliance culture within the organization.

For these reasons we positively evaluate the involvement of Compliance function in the hiring processes, assessing candidate inclination to compliance culture and providing feedbacks on the hiring decision.

Extending this line of reasoning toward hiring, we can infer that key positions should not be unaware of what compliance is: with main regard to Board of Directors, it is advisable that at least one of the board member should be formally skilled in compliance management.
Financial Services are crossing a fast changing environment from a technology standpoint, further reinforcing the need of Compliance to effectively predict events and manage information in a way that can provide a holistic and complete view of compliance health to key process owners and naturally senior management.

In particular, we see three main dynamics affecting the compliance complexity from such a perspective:

- **Rise of the ecosystem**: the landscape for conducting insurance is changing significantly, with globalization reducing transparency to suppliers, and utilities/cloud-based solutions meaning transactions may be supported by third, fourth, or even fifth parties. Let’s think as an example to the emerging role of specialized Fintechs as payment-service-providers, managing all the acquiring value-chain for premium collection and in some case outgoing payments: such an innovation open companies to increased risk of frauds and data capture via payment applications. As a consequence, understanding whom you are doing business with and who is supplying your organization will make predicting misconduct a reinforced capability;

- **Digitization**: new technologies, like cryptocurrencies and crowdfunding, are redefining how financial services firms do business globally and opening new communication channels that need to be managed. New ways of doing business will require compliance to rethink its control framework for keeping firms in compliance;

- **Structural reform**: global regulators are re-shaping firms to be more resilient through a series of structural reform regulations, necessitating review of products, client mix, and geographies to meet commitments for Returns on Equity. Compliance must leverage its “seat at the table” and demonstrate value as a strategic advisor in providing a complete view of compliance health as firms evolve.

As a starting point, our survey reveals that only few companies rank as excellent both their architecture and application landscape for compliance, not only in terms of simple automation, but also in terms of the key capabilities that enable predictions toward detection and mitigation. As a matter of fact, approximately 20% of the players surveyed revealed that they have integrated compliance/or compliance & risk architectures with ability to scale, whilst the vast majority still struggles with “scattered” architectures with poor ability to scale.

Going forward, compliance technology must harness disparate sources of data to provide meaningful insight, whilst also enabling critical controls that keep firms in compliance. Unified alert management layers are becoming more common for the compliance technology architecture, which also needs to support emerging disciplines such as behavioral analysis and social media surveillance.

![Figure 19. Conceptual IT Framework – Main Emerging practices](image)
As presented in Figure 20, several practices are emerging to boost compliance management:

- Sophistication in reporting, to detect ethical company health, favoring predictive approach;
- Use of big data and leverage on the power of analytics;
- Sophistication in technology dedicated to assess behaviors;
- Enlargement of control frameworks to include digital channels;
- Social media surveillance to understand use of corporate accounts and feedback;
- Common investigation layer to generate alerts

- One-top-shop portals for compliance officers and firm employees to monitor metrics and trends;
- Visualization tools to monitor communications and suspicious market behavior;
- Enterprise-wide capabilities to absorb all employee compliance information and facilitate data discovery.

All those trends are reflected into a new IT framework for compliance, able to embed new technologies, new techniques and new type of data (as showed in the next picture).
Looking at Figure 21 from the bottom to the top, we can decompose the architecture in four main layers:

- **Data collection layer.** Data collection can be both manual and automated: the main automated methods include ETL, APIs and batch processes both directed to Company internal systems and external data (e.g. social media, etc.);

- **Compliance engine.** Relational DB that through a Complex Event Processing (CEP) Engine connects risk information to regulatory requirements, business processes, controls, control owners and remediation tasks. Such a structured layer enables sophisticated analysis and reporting;

- **Workflow and alert manager.** Workflow engine manage approvals, reviews, assessments and investigations: the alert lifecycle allows setting of automatic controls/notifications addressed to the process owner;

- **Data delivery and reporting.** Output include automated reporting, communication with the internal and external stakeholders, portals update for compliance officers and firm employees to monitor metrics and trends.

Leveraging technology does not stop at setting up sophisticated architectures for non-compliance risk anticipation, detection and reporting: as a matter of fact, nowadays innovation in technology can be leveraged to support the journey of compliance towards the “collaborative” model without implying per se an increase of compliance costs, both internal (HR and Other administrative expenses) and external (new processes to be structured and put under control).

Moreover it should be considered that Compliance is one of the biggest consumers of data in the enterprise: it needs access to all of first line data as well as additional data to run its monitoring and surveillance.

The pursuit of an enterprise data lake is one solution firms are architecting, and Compliance functions are leveraging off these efforts rather than building their own. Therefore, Compliance needs to establish a relationship and leverage the expertise of a Chief Data Officer (or similar).

Our survey currently reveals that notwithstanding pressure on margins on the Companies and the increasing need for budget control, costs related to compliance management steadily increased and are planned to increase over the next three years (for ~70% of the respondents; of which 50% foresees a cost increase >10%).

On top of big data & analytics, in the short term we see major opportunities for Companies to leverage on RPA – “Robotic Process Automation” and Cognitive computing (samples are: clearance for research, information gathering to support KYC, …). These solutions help to effectively capture risks and control processes while keeping the cost of compliance under control:

- **RPA can be used to manage manual intensive/high-volume controls and to support investigation.** Let’s think about how time to deal with checks on contracts, underwriting procedures, product information templates can be dramatically reduced adopting a systematic robotized control approach; let’s think about how frequently controls can be run as patrols, giving statistical and material feedback to control owner and compliance team in case of any suspicious deviations. And again, let’s think how to easily track compliance training completion across your organization, especially in the case you are part of a multi-legal entity and multi-country company;

- **Machine learning systems enable computers to sense, comprehend and act with structured and unstructured data coming from different sources.** Imagine for a while how to connect regulatory tracking with impact analysis on key processes and control, leveraging on both pre-selected and adaptive rules to immediately locate where (at which activity and control level) a non-compliance risk is emerging, who is affected by, what are the processes affected and whether the controls should be added or modified.

One of the most significant advantages of RPA is its “speed to benefit” since it allows to realize efficiencies more quickly with respect to a multi-year big data program.

It is now not a matter of if, but a matter of when to exploit the potential of these tremendous breakthroughs.
Closing remarks

Regulatory pressure and insurance market dynamics have made Compliance a key function for the Board and for C-levels. CCOs are attempting to maintain grip on existing risks and controls, realizing meanwhile that a shift in the old paradigm “more risks, more controls, more people” is necessary to keep compliance affordable, without weakening the effectiveness of the framework.

Starting from our survey made on 15 of the largest insurance companies worldwide, we have seen material room for improvements, thus many opportunities for companies willing to rethink their operating model insisting on four main areas:

- **Control framework**
  Embedding a risk-based/principle-based approach in determining the boundaries of regulatory, legal and policies scope of the compliance would limit the probability of losing grip on the control itself. Techniques such as de-composition of balance sheet/P&L, combined with traditional “sanctionatory” approaches enable more focused oversight on non-compliance risk. Recurring regulations-processes mapping, despite its burden on the function during the setup phase, continues to be the key starting point of a sound framework.

- **Organization**
  Tuning between vertical and horizontal centralization, CCOs should find the best match for their organization. Integration with business and the right blend of “by risk type and by process type” models are the 2 key ingredients of an effective organizational deployment. Going forward companies should also explore further centralization through shared-services (also sharing resources across the industry), externalization on non-core activities or strong automation of highly repetitive and time-consuming tasks.

- **Processes**
  A simple 3-step approach is our suggested roadmap for an effective compliance functions in a context of increasing complexity and need for costs (direct and indirect) efficiency.
  - “Excel in core processes” means to enhance those activities that could guarantee full supervisory of non-compliance risks, also leveraging on an extended collaboration model involving third parties, and on technology (big data & analytics).
  - “Shift from risk mitigation to risk prevention” implies the full adoption of a risk-based approach in identifying key risks and controls, adopting a combination of traditional and more recent approaches that further involve business leaders as key control owners.
  - “Compliance culture infusion across the Company” means to bring the right awareness level on the importance of the Compliance within the firm. This also leveraging on both the internal communication/training lever but also on a sort of “total infusion” within the Company’s processes that could bring the Compliance to participate to hiring processes and to establish a compliance based incentive model.

- **Technology**
  Leveraging technology innovation in compliance does not simply mean to rethink current IT and application architectures trying to reduce at the utmost manual-intensive reporting and data flows. It embraces also to capture recent trends that are affecting the ecosystem, with main regard to robotics that allows cost reduction while keeping strict controls and cognitive computing to analyze and suggest effective actions to the control owners.

Excellence in compliance management is a product of two types of forces: those “traditional” impacting roles, responsibility, organization and processes, through which the Compliance management framework could be restructured in a direction of increased collaboration with business players; those driving innovation, through which also CCOs could enter and exploit the digital revolution reaching cost control and effectiveness.

The right mix of traditional and innovative forces will enable entering in the 2.0 space, rotating compliance management “to the new”.

30
Appendices

A1. Survey results factsheet

Although we have presented high level findings in this report, we have access to a far greater level of data from our survey and analysis. As an example here below we report a factsheet with some selected illustrations.

**Factsheet on Organization area results**

- **Is there a Chief Compliance Officer in your Group?**
  - 1 - No
  - 2 - CEO
  - 3 - CFO
  - 4 - CRO
  - 5 - General Counsel
  - 6 - Head of Organization
  - 7 - Other
  - 0 - None

- **What is the average working seniority of resources (employees) in your compliance function?**
  - 1 - Less than 6 years
  - 2 - Between 6 and 10 years
  - 3 - More than 10 years

- **Since when does the Compliance Function exist within your Company?**
  - 1 - > 10 years
  - 2 - > 5 years
  - 3 - < 5 years
  - 4 - Other

- **Does your Company leverage on a Shared Service in order to manage Compliance area processes?**
  - 1 - Yes
  - 2 - No

- **Are some of your compliance activities/processes externalized?**
  - 1 - Yes
  - 2 - No

- **Compliance function participation to committees**

31
Factsheet on Processes area results

Please check whether any of your company functions takes care of the following processes; detection of relevant laws and regulations impacting the company

- 1. Compliance Officer area
- 2. General Counsel area
- 3. Financial Officer area
- 4. Risk Officer area
- 5. Internal Controls (audit) area
- 6. Organization area
- 7. Other (please specify)
- 8. No function takes care of the process

Please check whether any of your company functions takes care of the following processes; analysis of relevant laws/regulations and mapping of how they impact processes/services of the company

- 1. Compliance Officer area
- 2. General Counsel area
- 3. Financial Officer area
- 4. Risk Officer area
- 5. Internal Controls (audit) area
- 6. Organization area
- 7. Other (please specify)
- 8. No function takes care of the process

Please check whether any of your company functions takes care of the following processes; overall monitoring on the compliance risk level within your organization

- 1. Compliance Officer area
- 2. General Counsel area
- 3. Financial Officer area
- 4. Risk Officer area
- 5. Internal Controls (audit) area
- 6. Organization area
- 7. Other (please specify)
- 8. No function takes care of the process

Please check whether any of your company functions takes care of the following processes; reporting vs top management about compliance risk level

- 1. Compliance Officer area
- 2. General Counsel area
- 3. Financial Officer area
- 4. Risk Officer area
- 5. Internal Controls (public) area
- 6. Organization area
- 7. Other (please specify)
- 8. No function takes care of the process
Factsheet on IT area results

What best describes your compliance IT architecture? (level of integration is intended as the degree of integration between the compliance IT system and the various internal IT systems of the other company functions)

- 63% Not integrated and standalone IT solutions for compliance
- 26% Some integration of the compliance infrastructure and some standalone solutions
- 13% Integrated compliance infrastructure with ability to scale
- 13% Integrated compliance and risk infrastructure with ability to scale
- 13% No IT system in place

How much automated overall are compliance processes in your function?

- 67% Very Much Automated
- 40% Good bled with some areas of improvement
- 7% Poorly Automated
- 7% Not automated at all
- 7% Other

Does your Company adopt a Big Data solution to manage Analytics? (If yes, please specify in the comments field)

- 87% Yes
- 13% No

Does your Company adopt an IT system based on Analytics? (If yes, please specify in the comments field)

- 50% Yes - a deterministic model in order to manage current risks and prevent associated losses
- 47% Yes - a predictive model in order to foresee tomorrow’s hidden risks and prevent them
- 47% Yes, both deterministic and predictive models
- 47% No

Which of the following processes are completely and appropriately supported by IT systems/External Services (if available)

1. Detection/Collection, Synthesis and Propagation of Relevant Laws and Regulations Impacting the Company
2. Analysis and Mapping of Relevant Laws and Regulations with the Multiple Processes Areas of the Company
3. Overall Monitoring on the Compliance Risk Level within your Organization
4. Reporting vs Top Management about Compliance Risk Level
5. Assessment of Current Processes/organization Structure in Order to Verify their Adequacy with respect to New...
6. Identification and Activation of the Initiatives to Address the Noncompliant Areas Identified...
7. Initiatives Follow-up of the Initiatives Launched to Address the Noncompliant Areas Identified in the Compliance Risk Assessment...
8. Proactive Compliance Risk Mitigation and Prevention through the Launch of Detailed Initiatives that Anticipate Potential New...
9. Management of the Relation with the Supervisory Authority and/or Regulators
10. Advisory to Business Lines and Top Management on Compliance Matters
11. Training on Compliance-related Matters to Resources of 1st Line Functions (QO, Underwriting, Pricing, etc.)
12. Internal Regulatory Development and Management (Definition of Internal Controls of Their Implementation...)

*...1.2%"
A2. Survey panel and methodology

Methodology

Our survey was designed to understand the current shape and the outlook trends for the Compliance Management within the overall organization and operating framework of the Insurance industry. This survey was conducted mainly by personal interviews with the Chief Compliance Officers or other direct representatives from the Compliance function of each Insurance Company involved. When preferred by the Company, also a direct response through an autonomous fulfillment of questionnaire was accepted. The panel has been selected including Companies from Italy, France, Germany, Spain, Japan, UK, Luxembourg and USA (see interviewed panel features here below). Questionnaire was based on 150 questions (of which 55 “mandatory”) aimed to investigate the Compliance functions Target Operating Models around these pillars:
- Company profile (general data)
- Organization
- Processes
- Technology
- Trend and outlook

Interviewed panel
About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders.

With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Contact the authors

To learn more about how Accenture can help your organization, please contact the authors:

**Niccolò Bergamini**
Managing Director – Italy, Central and Eastern Europe and Greece F&R Insurance Lead
niccolo.bergamini@accenture.com

**Paolo Mazzer**
Senior Manager - F&R Insurance
paolo.mazzer@accenture.com

**Matteo Romanò**
Manager - F&R Insurance
m.romano@accenture.com

**Anna Benetto**
Manager - F&R Insurance
anna.benetto@accenture.com

Accenture Finance & Risk practice

Accenture F&R is a practice with more than 5,000 professionals across the world (350+ in Italy) working with leading Financial Services clients to address the Finance & Risk agenda through this suite of services: Regulatory & Compliance, Finance & Accounting, Cyber Risk & Resilience, Sourcing & Procurement, Financial Risk Management, Finance & Risk Analytics.

Within Regulatory & Compliance service, Accenture boasts a practice focused on innovating and transforming the Compliance function for Insurance players combining:
- Strong industry knowledge
- End-to-end capabilities (leveraging consulting, digital and technology and operations services)
- Global Network
- Assets and accelerators

Finance and Risk key contacts for Insurance Industry:

**Eric Jeanne**
Managing Director – Global and France, Netherlands, Belgium and Luxembourg F&R Insurance Lead
eric.jeanne@accenture.com

**Markus Salchegger**
Managing Director – Europe, Middle East, Africa and Latin America and Austria, Switzerland and Germany F&R Insurance Lead
markus.salchegger@accenture.com

**Christopher Johnston**
Managing Director – North America F&R Insurance Lead
c.b.johnston@accenture.com

**Masaharu Akasaka**
Managing Director – Asia Pacific F&R Insurance Lead
masaharu.akasaka@accenture.com

**Laurent Gautlier**
Managing Director – Global Technologies F&R Insurance Lead
laurent.gautlier@accenture.com

**Niccolo Bergamini**
Managing Director – Italy, Central and Eastern Europe and Greece F&R Insurance Lead
niccolo.bergamini@accenture.com

**Adriano Regis**
Managing Director – Latin America F&R Insurance Lead
adriano.regis@accenture.com

**Duncan Bernhard**
Managing Director – North America F&R Insurance Lead
duncan.barnard@accenture.com

**Tales Lopes**
Managing Director – Denmark, Northway Sweden and Finland F&R Insurance Lead
tales.s.lopes@accenture.com

**Antonio Fernandez Garcia**
Managing Director – Spain and Portugal F&R Insurance Lead
a.fernandez.garcia@accenture.com

**John Morley**
Managing Director – United Kingdom and Ireland F&R Insurance Lead
john.b.morley@accenture.com

Join the conversation

Twitter
Accenture

LinkedIn
Accenture Finance & Risk Services

Website
http://financeandriskblog.accenture.com/

Copyright © 2016 Accenture
All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.