CHAPTER 9

Compliance Risk Management

"The secret of getting ahead is getting started."

—Mark Twain

"Nothing will ever be attempted, if all possible objections must be first overcome."

—Samuel Johnson

The purpose, in simple terms, of risk management is to protect *all* of the stakeholders of an organization with a predominant bend toward customer/client/consumer protection. A point to note is that protection of *all* stakeholders is the purpose of effective risk management. So while the traditional risk areas like credit, market, and operational risk endeavor to protect the solvency, profitability, liquidity, and growth of the organization, the environmental requirements manifested as laws, regulations, or market expectations seek to protect customers, market, and the economy they operate in, in addition to the organizations themselves.

There are times when there could be conflict of interest between the narrowly defined organizational objectives and the environmental expectations from it. The reason I say "narrowly defined" objectives is because in its true spirit there is no conflict as the organizational objective at its fundamental level is to have "sustained growth," which is really possible only when all the stakeholders' well-being is ensured. A distinction needs to be made between the organization as a legal person by itself and its management at a point in time. They are not necessarily synonymous. This aspect is discussed in Part Five of the book on real-life issues of compliance management. Controls are an integral and core component of risk management. The

Enterprise Compliance Risk Management: An Essential Toolkit for Banks and Financial Services.
Saloni P. Ramakrishna

objective of controls is to prevent risk or in the event it does manifest to minimize the impact.

A compliance risk management program, to be effective, needs to be able to proactively anticipate the potential events that may affect the organization and set in place a mitigation and management process that is based on its business model, objectives, risk appetite, and strategic direction within the context of its environment, as reflected in the current and anticipated market, economic, and competitive landscape.

RISK APPETITE

Can an organization have an appetite for compliance risk? Can there be any such thing as an organization implying that it could disregard the laws or regulations? Compliance and the honoring of the boundaries set by the organizational environment are expected. While the actual penalty of the minor violations might be insignificant, the ramifications of what is seen as wilful disregard of laws and regulations could be painful in both the medium and long run. Organizations are faced with the paradoxical situation of an expectation of strict compliance and the impracticality of zero slippages.

Is it possible to articulate a risk appetite statement for compliance risk? This is an interesting question. The challenge is that theoretically and ideally there needs to be zero appetite for compliance risk, but in reality that is not possible. How does an organization articulate its compliance risk appetite? I posed this question to a few of my C-level friends. Many of them said they do not specify any risk appetite for compliance risk, as the implicit understanding is zero tolerance to compliance slips. Not making specific reference to zero appetite to compliance risk is practical; one of them reasoned with me that it helps manage minor non-serious compliance slips. My counter-question was, why not make that a part of the appetite statement? State that you have low appetite and have effective controls in place to manage the same? This might not be acceptable to the regulators and auditors, they countered. One of the more experienced CROs from one of the developed economies said they have stated in their policy statement that they have zero tolerance for *immediate nonreporting* of compliance breaches. His reasoning was it is unrealistic to think there would be no breaches; the greater risk stems from nonreporting of the same, which will impair immediate remedial actions. This sounded very practical and prudent. This approach helps early identification of risks and therefore early arrest/mitigation of the impact of noncompliance on the one hand, and if it is a learning organization, it can be translated into strengthening of the control processes to arrest reoccurrence of similar breach on the other. Categorizing and communicating the risks of noncompliance and the low/no-risk appetite to all concerned helps set right expectations.

RISK IDENTIFICATION

Early identification of risks is critical to the success of compliance risk management. A corporate directive of zero tolerance to immediate nonreporting of compliance breach discussed earlier, though reactive, is certainly an effective step. An active and positive management puts in place a proactive risk identification process.

The possible approaches of proactive identification would, at the minimum, require two inputs: the compliance risk classes or genres and the risks identified that are generated through the risk identification tools. Figure 9.1 reflects compliance risk classes or blocks as discussed earlier in Chapter 6 (Figure 6.5).

The broad classes or genre are:

- Financial crime/abuse of financial system
  - Money laundering—connected requirements: AML (Anti–Money Laundering) and KYC (Know Your Customer)
  - Terrorist financing—connected compliance requirement: CFT (Combating the Financing of Terrorism)
  - Tax evasion example of connected requirements: FATCA (Foreign Account Tax Compliance Act)
- Fair treatment of customers—example: "mis-selling"
- Customer/market disclosures—example: MiFID
- Safety and soundness of the system——example: Basel norms, antitrust requirements

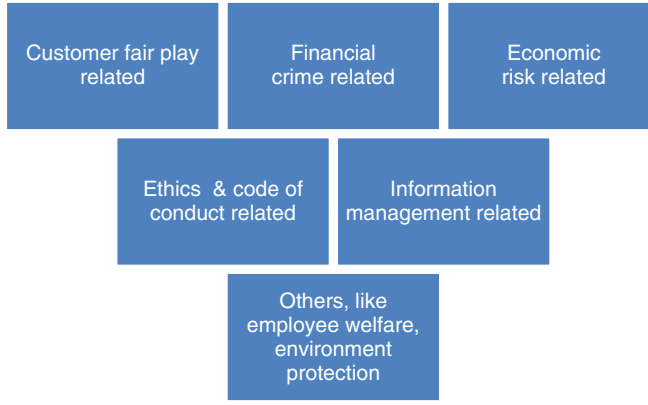

FIGURE 9.1 Compliance Risk Classes or Blocks

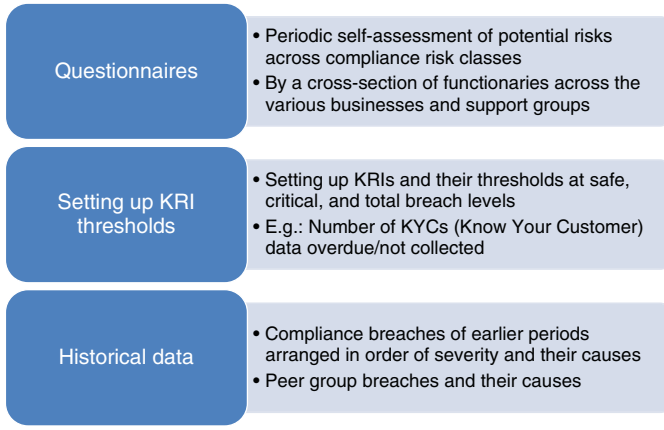

FIGURE 9.2 Compliance Risk Identification Tools

TABLE 9.1 Risk Identification Map

Geography Name	Financial Crime/ Financial Abuse	Fair Treatment of Customers	Market Disclosures	Systemic Requirements	Code of Conduct
Retail Banking	High Risk	Medium Risk	Low Risk	Medium Risk	Low Risk
Corporate Banking	High Risk	Low Risk	Low Risk	Medium Risk	Low Risk
Insurance	Medium Risk	High Risk	Medium Risk	Medium Risk	Medium Risk
Capital Market Operations	Low Risk	High Risk	High Risk	High Risk	Low Risk
Information Technology	Low Risk	Low Risk	Medium Risk	Medium Risk	Medium Risk
Human Resources	Low Risk	Low Risk	Low Risk	Low Risk	High Risk
Other Support Functions	Low Risk	High Risk	High Risk	Medium Risk	High Risk

Figure 9.2 shows a sample of risk identification tools.

Plotting the potential of risks across various blocks as identified through the risk identification tools against each line of business produces the risk identification maps. A sample is given in Table 9.1.

Note that this is not a sample of organizational level report or a risk map for compliance. It is a sample for a particular geography risk profile. It denotes the risk status at a point in time. It helps firms understand where to focus their attention in the concerned geography. The aggregation of this

map to an organizational level can take the scorecard building approach by assigning weights to the three dimensions used here, which are geography, line of business, and the compliance risk genre (building a scorecard is dealt with in some detail under the risk assessment section). The information can then be used to slice-and-dice the profiles in multiple ways. For example, a risk map can be created by risk genre or by LOB. Some samples can be seen in Tables 9.2 (by Risk Genre) and 9.3 (by LOB).

Capturing periodically point-in-time snapshots and comparing them across time helps understand whether there is an improvement of the risk profile. A sample is given in Table 9.4 for a given risk genre and geography across LOBs.

Analysis of Table 9.4 shows that there is status quo of low risk in IT, improvement in retail banking, dramatic improvement in corporate banking, and negative effect under insurance and a slide down in the capital markets without the need for detailed writeups and wordy slides.

These sorts of data-based dashboards help present the risk picture to management and regulators in a simple yet comprehensive manner. Technology is a big enabler in this space.

TABLE 9.2 Geography View across Financial System Abuse

Financial Crime/Financial Abuse	Geography 1	Geography 2	Geography 3
Retail Banking	High Risk	Medium Risk	Low Risk
Corporate Banking	High Risk	Low Risk	Low Risk
Insurance	Medium Risk	High Risk	Medium Risk
Capital Market Operations	Low Risk	High Risk	High Risk

TABLE 9.3 Sample of LOB (Line of Business View)

Retail Banking	Financial Crime/Financial Abuse	Fair Treatment of Customers	Code of Conduct
Geography 1	High Risk	Medium Risk	Low Risk
Geography 2	High Risk	Low Risk	Low Risk
Geography 3	Medium Risk	High Risk	Medium Risk
Geography 4	Low Risk	High Risk	Low Risk

TABLE 9.4 Comparison of Risk Profile across Two Time Periods

For—Geography Name	Financial Crime/Financial Abuse at Time *X*	Financial Crime/Financial Abuse at Time *X* + 1
Retail Banking	High Risk	Medium Risk
Corporate Banking	High Risk	Low Risk
Insurance	Medium Risk	High Risk
Capital Market Operations	Low Risk	High Risk
Information Technology	Low Risk	Low Risk

Areas of Concern

RISK ASSESSMENT

"What cannot be measured cannot be managed."
—W. Edwards Deming

In the area of compliance risk, firms have or are expected to have zero tolerance for compliance risk breaches. Periodic and proactive assessment of risks being assumed becomes critical. The stakes here are very high. In traditional risk areas like credit and market, money is at risk; but in compliance, business is at risk. It can be argued at the end of the day that all risks get translated into financial statistics, but this could go beyond just numbers. A methodical process as in Figure 9.3 is vital for the success of the compliance risk management program.

Risk assessment is not a simple arithmetic problem to be solved but a methodical approach of gathering, organizing, and analyzing data in such

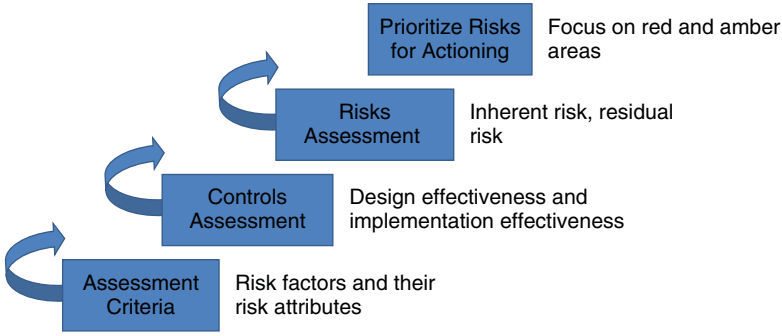

FIGURE 9.3 Compliance Risk Assessment Process

a way that it gives meaningful and near-realistic indication of the risk that is being carried. The basic themes that need answers are what can possibly go wrong; what is the possibility that they actually can go wrong; and, if they do, what is the potential impact. The answers to these questions help management to decide how these risks can be mitigated/managed. The real job of risk assessment/measurement is to provide accurate estimates of the risks being carried. The management armed with these inputs decides on the trade-offs between the costs and value of the various options open to it from risk acceptance to risk avoidance. Again, given that this discussion is in the context of compliance risk, managements tend largely toward risk avoidance.

At the top level there are two components that go to build a risk assessment framework. They are quantitative aspects and qualitative aspects. Typically, a hybrid is used where qualitative aspects, which lend themselves to conversion to quantitative attributes for the purposes of assessment, are preferred.

Quantitative Aspects of Compliance Risk

The number of incidents of compliance breaches, amount of fines levied in a given period, number of strictures, complaints, amounts identified under insider trading, and fraud are some examples of quantitative indicators. The firm, based on its business model, nature of business operations, and geographies it operates in, can set up the thresholds of low, medium, and high (or a five-point scale as appropriate) classifications. What needs to be kept in perspective while doing so is the fact that these thresholds are being set up for compliance risk where the risk tolerance is very low. The definition and thresholds have to be recorded in the compliance policy. This helps in two ways: First, there will be uniform understanding across the organization; second, it is easy to explain to the regulators/auditors and other lawmakers and prove beyond doubt that there is no arbitrariness in how they are defined or used in downstream assessment processes. Here is an example:

- **Low**—Compliance breaches less than "X" and between criticality rating 8 to 10 (if criticality ratings are on a 10-point scale with 10 being the lowest) or criticality rating 5 (if criticality ratings are on a 5-point scale)
- **Medium**—Compliance breaches between "X and Y" and between criticality rating 5 to 7 (if criticality ratings are on a 10-point scale) or criticality rating 4 (if criticality ratings are on a 5-point scale)
- **High**—Compliance breaches above "Y" and between criticality rating 1 to 4 (if criticality ratings are on a 10-point scale) or criticality rating 1 to 3 (if criticality ratings are on a 5-point scale)

Qualitative Aspects of Compliance Risk

The quality of compliance is reflected in terms of the effectiveness of controls, the compliance risk history, and the alignment of management and board with the compliance program. The typical three-point structure can be as follows:

- **Strong**—Visible management commitment, well-defined compliance program with clearly laid out responsibility and accountability. Good systems and procedures in place. No/minimal negative comments on compliance program and its implementation by regulators, auditors, and other lawmakers. Controls well defined and executed.
- **Adequate**—Management empathetic but reactive, good compliance program with clearly laid out responsibility and accountability but not as strong on implementation of the program. Systems and procedures in place but not very well coordinated. Few negative comments on compliance program and its implementation by regulators, auditors, and other lawmakers. Controls well defined and not so well executed.
- **Needs improvement/weak**—Management views compliance as a cost function and therefore looks at it as a checkbox function. Systems and procedures created as a response to a requirement and on ad-hoc basis. Many (and a few really serious) negative comments, strictures on compliance program and its implementation by regulators, auditors, and other lawmakers. Fines and penalties levied. Controls ill defined and executed.

A combination of both, status of compliance culture and implementation effectiveness, shows the compliance risk status of the firm. For example, a strong compliance culture and implementation results in low compliance risk and low quantitative impact. A weak compliance culture on the other hand more often than not results in high compliance risk and the resultant high cost.

Assessment Methods

Compliance risk models are largely scorecard based. Scorecarding is a popular method resorted to for compliance risk assessment because of the nature of the risk, data availability, and the nascent stage of academic study on stochastic modeling in this field. Having said that, it needs to be pointed out that there could be exceptions like the models that are found within some subareas of compliance like the anti–money laundering space. The customer risk scoring models for customer due diligence and extended due diligence are examples. However, when one is looking at compliance risk assessment in a holistic fashion, then it is more the scorecarding procedure that is resorted to.

It is interesting to note that while statistical options are at a nascent stage in the financial services compliance risk, its modeling and measurement is well advanced in industries like tax compliance, health, and pharmacy. This is so because these industries have been tracking compliance and compliance data for a long time.

The purpose of scorecard building is to understand the compliance risk that the organization carries at an aggregated level as well as at a detailed level, allowing deep dives into areas of concern. The question often asked is how involved the scorecard or model needs to be. It is important to note that *building the model is not an end in itself. It is not built for the modeler. It is for use by business to get insight into the risks they are carrying in a simple, clear, and understandable manner, so they can act on it and prevent/mitigate the risks*. It is how it lends itself to business objectives, its serviceability, and maintainability that are vital inputs to designing a model. Where one draws a line in the analysis process without getting into the "paralysis by analysis" syndrome is determined by considering five fundamental features:

- Objective of the exercise—in this case, to assess compliance risk of the firm
- Data/input availability—what is the granularity of relevant data/input available and what is its reliability
- Ability to facilitate aggregation and disaggregation to support macro-view and micro-correction
- Simple to understand and lend itself as a meaningful input to decision makers
- Operationally robust

Some firms include compliance risk in operational risk computations. It gets rolled up into the overall operational risk assessments and measurements with compliance risk events considered events with severity and frequency data. Stand-alone statistical modeling of compliance risk is still at its nascent stages owing to the nature of events and availability of sufficient data points to make an intense statistical method reliable, robust, and relevant. However, there is no mistaking the fact that scorecards fall under the umbrella of models. "The definition of model also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature."[1]

[1] "Supervisory Guidance on Model Risk Management," Board of Governors of the Federal Reserve System Office of the Comptroller of the Currency, April 2011.

"A model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three components:

- An information input component, which delivers assumptions and data to the model
- A processing component, which transforms inputs into estimates, and
- A reporting component, which translates the estimates into useful business information"[2]

One of the most important tools in compliance risk assessment and measurement can be scenario analysis. The scenarios can be across the spectrum right from a BAU (Business as Usual) scenario to a stress/worst-case scenario. Financial services firms are facing a spate of fines and penalties, more since 2012. Each of the headlines-grabbing fines/penalties can be defined as one scenario. Risk and control effectiveness can then be reassessed in the backdrop of the scenario. Like I mentioned earlier in the book, in compliance risk not just complying but being able to demonstrate compliance is important. Regulatory scrutiny today is taking action not only for actual events but also for lack of robust measures to arrest the possibility of occurrence of an event, as a preventive measure.

Understanding the vulnerability of the organization is critical to managing the volatile regulatory and market environment. *Assessment of velocity or speed with which an event can impact the firm* is another facet that needs to be kept in perspective. Scenario analysis need not be just blue-sky thinking; firms can pick up on the real-life experiences of their peers and model their scenarios by asking the "what-ifs": How prepared is their firm both in preventing such situations and support if a similar verification/scrutiny was done. This will help them assess their readiness to handle similar situations. Modeling a real-life event from peer group experience helps plug the loopholes if any in the processes or controls where they exist or put in place controls where they do not exist.

Inherent Risk and Its Assessment COSO defines inherent risk as "the risk to an entity in the absence of any action management might take to alter either the likelihood or impact."[3] Inherent risks are risks that are present

[2]Ibid.
[3]COSO Enterprise Risk Management—Integrated Framework (2004).

and are similar across the firms of the same industry. Note I have said "similar" but not "same" because depending on the business model, business practices, and the countries of operation, the same regulation could translate into different magnitudes of inherent risks for different firms. Inherent risk is expressed as the sum of impact and likelihood (probability).

$$\text{Inherent risk} = \text{Impact} \times \text{Likelihood}$$

The examples in Tables 9.5a, 9.5b, and 9.5c take simplistic representations of three values for impact and likelihood—a three-by-three matrix. The impact and likelihood can be computed using either questionnaires or historical data (of self or peer group or both) logically segmented.

Translating the inherent risk to a heat map would look like Table 9.6.

If the firm wants to have a more fine-grained segmentation or classification, then cells 5 and 10 (grouped into Low in Table 9.6) can be divided into two classes instead of one as insignificant (5) and low (10). Similarly 15 and 25 can be classified into two segments and so on. The purpose here is to understand the inherent compliance risk and develop appropriate controls. The design construct can be modified to suit the data availability and reliability on an ongoing babsis as well as the organizational complexity.

TABLE 9.5a
Impact Scale

Impact	
Low	1
Medium	5
High	10

TABLE 9.5b
Likelihood Scale

Likelihood	
Unlikely	5
Possible	10
Very likely	15

TABLE 9.5c Inherent Risk Computation

Impact	Likelihood	Inherent Risk
10 (High)	15 (Very Likely)	150
5 (Medium)	10 (Possible)	50
1(Low)	5 (Unlikely)	5

TABLE 9.6 Heat Map of Inherent Risk

Inherent Risk				
		Impact		
		Low	Medium	High
Likelihood	Unlikely	5	25	50
	Possible	10	50	100
	Very Likely	15	75	150

Controls and Their Assessment One of the critical aspects of managing compliance risk is the nature and effectiveness of controls. Given the inherent compliance risk, firms put in place controls to mitigate it. Control effectiveness has two aspects, the design aspect and the implementation aspect. The overall impact/efficiency of controls is a result of combined effect. On a general note it can be said that while both aspects are important, the design effectiveness is more stabilized. It is the implementation effectiveness that needs sharper focus both in terms of actual implementation and measure. Periodic assessment of control efficacy is critical for the success of the firm's compliance program.

$$\text{Control effectiveness} = \text{Design effectiveness} \times \text{Implementation effectiveness}$$

Here, too, it is a three-by-three matrix with the two dimensions being design and implementation effectiveness. The values for these two dimensions can be sourced from questionnaires/historical data/audit reports. If there are good systems and good data, these values can be derived as well. The scale can be 3, 5, or any number that the organization is confident of maintaining on an ongoing basis.

A simple control assessment sample on a scale of 3 as in Tables 9.7a, 9.7b, and 9.7c has effective, moderate, and weak as the three aspects.

As mentioned earlier more depth and detail can be added to each of the dimensions. For example, on the design side further detail can also be built in for strong and unified IT systems, proactive/reactive review cycles, and so on. On the implementation side details can be control breakdowns,

TABLE 9.7a Design Effectiveness Scale

Design Effectiveness	
Weak	1
Moderate	5
Effective	10

TABLE 9.7b Implementation Effectiveness Scale

Implementation Effectiveness	
Weak	1
Moderate	5
Effective	10

TABLE 9.7c Heat Map of Control Assessment

Control Assessment				
		Implementation Effectiveness		
		Effective	Moderate	Weak
Design Effectiveness	Effective	100	50	10
	Moderate	50	25	5
	Weak	10	5	1

compliance breaches (in spite of the controls), ease of implementation (or the lack of it), and so on.

Residual Risk and Its Assessment Armed with inherent risk and control assessment, the next step is to arrive at the residual risk. From an assessment point of view, the practice is to assess inherent risk, controls, and the residual, which is expressed as inherent risk divided by controls.

$$\text{Residual risk} = \text{Inherent risk} \div \text{Control effectiveness}$$

From the illustrative values in Table 9.7 the residual risk metric (of dividing inherent risk numbers by the control effectiveness numbers) will range from 0.05 all the way up to 150. Banding the resultant residual risk numbers into 3, 4, or 5 scales (percentile or simple sorting and banding can be used), as in Table 9.8, of high residual risk, medium residual risk, low residual risk, will present the picture of residual risk.

Compliance Risk Fitness Barometer Assessment Critical to the exercise is not the mechanics of building a heat map. The two aspects that lend meaning to the heat map and its interpretation are the attributes selected and the weights

TABLE 9.8 Template for Residual Risk

	Inherent Risk	Control Effectiveness	Residual Risk
Financial Crime and Compliance			
Fair Treatment of Customers			
Systemic Risks Related			
IT Related			
Ethics and Conduct Related			

assigned for the purposes of aggregation such that it is a true reflection of the assessments. Management will be making a decision based on the heat map and its explanation by the compliance team. Hence, utmost care needs to be taken in its design and build. *The interpretation of the numbers is as vital as building a credible scorecard.*

The idea really is to measure and convey the health (or the lack of it) in a simple, understandable way. Continuing with our example, the output of residual risk computation in the form of high, medium, and low for the various risks is an input into the fitness computations. The next step would be to arrive at a weighted average of the risks in various categories. Notice here the number of risks in each of the categories and weights assigned (Based on the risk—higher the risk metric, higher the weightage) to each combination. The weighted average when converted into percentage provides the risk indicator or index; 100 (full fitness score) minus the risk index will give a "fitness barometer." The financial crime component is the sample used in Table 9.9 for illustrating the point.

TABLE 9.9 Compliance Risk Fitness Barometer

	No. of Risks	Weightage	Weighted Values
High/Strong	6	1%	0.06
Medium/Moderate	3	50%	1.5
Low/Weak	1	100%	1
Total	**10**		**2.56**
Total weighted values/total risks (2.56/10)			0.256
Risks indicator expressed as a percentage			25.6
Compliance risk fitness barometer (100 – 25.6) Full fitness score out of 100			74.4

TABLE 9.10 Sample of Residual Compliance Risk Report

Residual Risk Report	For LOB or for Geography			
	Number of Risks	Number of Controls	Residual Compliance Risk Indicators (RI)	Fitness Barometer
Financial crime and compliance Data from the earlier example	10	3	25.6	74.4
Fair treatment of customers				
Systemic risks related				
IT related				
Ethics and conduct related				

This process can then be used to aggregate an individual compliance area or across geographies or lines of business or any other meaningful aggregation structures. The sample of residual compliance risk report can be seen in Table 9.10.

Detailed Example of Compliance Risk Scorecard

The previous section illustrates how inherent and residual risk for different functional areas by LOB or by geography can be arrived at. The illustration in this section looks at the process of building a compliance risk scorecard with an example:

The process flow followed is detailed in Figure 9.4.

Table 9.11 captures the risk factors and their risk attributes used in the sample. Level one is the overall compliance risk. Level two is the components or the risk factors, which are broadly divided into six aspects (row one of the table). Notice that this is a different view of compliance risk assessment. The focus for this scorecard is assessment across the organizational risk factors. At level three each of these risk factors are then detailed into risk attributes that represent each of these risk factors. Sample risk attributes for each of these risk factors (rows 2 to 5) can be seen in Table 9.11.

The three levels here are illustrative. If data is available or the next levels of detail can be meaningfully built, then it can go up to five levels as well.

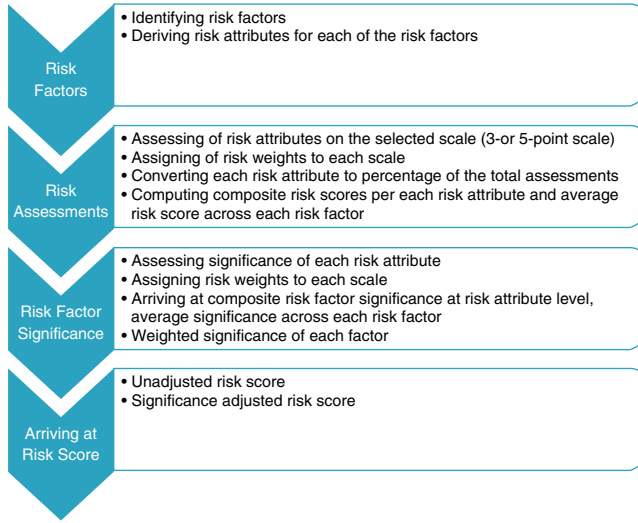

FIGURE 9.4 Compliance Risk Scorecard Build Flow

For example, shareholders' complaints score can be derived from assessing the nature, severity, and number of complaints. Once the risk factors and their underlying risk attributes are firmed up, then the actual building of the scorecard (or the actual assessment) begins.

Typically, there are two ways to get relevant risk attributes similar to the ones we discussed in the earlier example. One is the questionnaire method where a *simple and brief* questionnaire is administered to the *relevant and representative* internal stakeholders. I have highlighted two vital aspects of questionnaires both of which together will make the exercise meaningful. The other is to peg some real-life metrics to each of the risk attributes. The challenge could be the availability of data for all the risk attributes. Where available it would be good to use these metrics. A few examples can be seen in Table 9.12.

The sample scorecard being built here is based on the questionnaire method; the structure could easily be used for data-based build as well since both the inputs are at the leaf level after which the scorecards run on the aggregations logic. Based on either the questionnaire responses or the actual data, the data is classified as low, medium, or high risks and plotted against each of the risk attributes as shown in Table 9.13.

TABLE 9.11 Building a Scorecard

Organization	Management	Compliance Risk Risk Factors ↓ Business Practices	Employee	Customer	Third Party (Outsourcing)
Market abuse	Breach of code of conduct	Misleading marketing and mis-selling	Breach of code of conduct	Not giving or misrepresenting KYC details (Know Your Customer)	Complaints against the outsourcing partners/vendors
Nondisclosures, incorrect or incomplete disclosures to all stakeholders including regulators	Conflicts of interest in terms of roles within the organization or outside positions held	Irregularities in product and services offered Risks costs	Acceptance or giving of bribery in the form of gifts, favors	Abuse of financial system Money laundering Terrorist financing Tax evasion	Conformance to regulations and standards expected
Shareholders' complaints to regulators	New products/ services without proper governance structures	Advisory services (improper or misleading)	Insider Trading	Misrepresentation of facts	Security and privacy issues
Negative press for regulatory breaches	Insider trading	Customer complaint management	Fraud	Improper transactions	Continuity of services

TABLE 9.12 Metrics for Each of the Risk Attributes

Risk Attribute	Frequency	Severity
Customer complaint management	Number of complaints by quarter	Number in top three levels of criticality
Shareholders complaints to regulators	Number of complaints by quarter	Number in top three levels of criticality
Regulatory breaches	Number of breaches by quarter	Fines and penalties levied
Insider trading	Number of times insider trading identified	Fines and penalties levied
Bribery	Number of bribery cases by quarter	Amount

Table 9.13 captures the risk assessment tabulation against each risk attribute based on the questionnaire output/data. Total questionnaire count in the example is set at 20.

These are then converted into percentages using a simple relationship of number of data points to the total. Adding to this the weightage of each risk category, we took 1, 2, and 3 as weights for low, medium, and high risks respectively. With this we now have two important intermediary values:

- Risk expressed as a percentage against each risk attribute
- Weightage attributed to each risk class: low, medium, and high

Using both, we can compute the *composite risk score* for each attribute. This is then averaged out at the risk factor level to arrive at the composite risk score at the risk factor level as shown in Table 9.14. The risk attribute scores can be averaged out using a simple average or a weighted average if appropriate and reliable weightages can be arrived at.

Once composite risk score of each risk factor/attribute is available, the next step is to assign the relative significance of each risk attribute and arrive at the significance-adjusted composite risk score. Significance factor is arrived at by adopting the same method of weighted value of the significance of data (as detailed in Tables 9.13 and 9.14 using significance of the risk attribute as the metric, based on questionnaire output/data). The resultant table that shows the risk factor significance at the attribute level and averaged at the risk factor level is Table 9.15.

TABLE 9.13 Example of Compliance Risk Scorecard

Compliance Risk				
Risk Factors and Risk Attributes				
1. Business practices related				
	LOW RISK	MEDIUM RISK	HIGH RISK	Total Assessments
Inappropriate Marketing Practices, Sales practices (mis-selling)	8	10	2	20
Irregularities in Product and Services offered	10	8	2	20
Advisory services (improper or misleading)	12	7	1	20
Customer complaint management	14	6		20
New Product Implementation	10	6	4	20
2. Organization related				
Market abuse	11	8	1	20
Nondisclosures, incorrect or incomplete disclosures to all stakeholders including regulators	13	7	0	20
Shareholders' complaints to regulators	9	10	1	20
Negative press for regulatory breaches	10	7	3	20
3. Management related				
Breach of code of conduct	11	9		20
Conflicts of interest in terms of roles within the organization or outside positions held	12	7	1	20
New products/services without proper governance structures	14	6		20
Insider trading	7	9	4	20

(*continued*)

TABLE 9.13 (*Continued*)

Compliance Risk				
4. Employee related	LOW RISK	MEDIUM RISK	HIGH RISK	Total Assessments
Breach of code of conduct	10	10	0	20
Acceptance or giving of bribery in the form of gifts and favors	12	8	2	20
Insider trading	16	4	0	20
Fraud	6	10	4	20
5. Outsourced third party related				
Complaints against the outsourcing partners/vendors	13	7	0	20
Conformance to regulations and standards expected	12	6	2	20
Security and privacy issues	18	2	0	20
Continuity of services	11	6	3	20
6. Customer related				
Not giving or misrepresenting KYC details (Know Your Customer)	12	8	0	20
Abuse of financial system Money laundering Terrorist financing Tax evasion	12	6	2	20
Misrepresentation of facts	16	4	0	20
Improper transactions	6	8	6	20

TABLE 9.14 Example of Compliance Risk Scorecard

Compliance Risk				
	Risk Weights			
Risk Factors and Risk Attributes	1	2	3	
1. Business Practices related				Composite Risk Score
	LOW RISK	MEDIUM RISK	HIGH RISK	
Inappropriate Marketing Practices, sales practices (mis-selling)	40.00%	50.00%	10.00%	1.7
Irregularities in Product and Services offered	50.00%	40.00%	10.00%	1.6
Advisory services (improper or misleading)	60.00%	35.00%	5.00%	1.45
Customer complaint management	70.00%	30.00%	0.00%	1.3
New product implementation	50.00%	30.00%	20.00%	1.7
2. Organization related				1.55
	LOW RISK	MEDIUM RISK	HIGH RISK	
Market abuse	55.00%	40.00%	5.00%	1.5
Nondisclosures, incorrect or incomplete disclosures to all stakeholders including regulators	65.00%	35.00%	0.00%	1.35
Shareholders complaints to regulators	45.00%	50.00%	5.00%	1.6
Negative press for regulatory breaches	50.00%	35.00%	15.00%	1.65
3. Management related				1.53
	LOW RISK	MEDIUM RISK	HIGH RISK	
Breach of code of conduct	55.00%	45.00%	0.00%	1.45
Conflict of interests in terms of roles within the organization or outside positions held	60.00%	35.00%	5.00%	1.45
New products/services without proper governance structures	70.00%	30.00%	0.00%	1.3
Insider trading	35.00%	45.00%	20.00%	1.85

(*continued*)

TABLE 9.14 (*Continued*)

Compliance Risk				
	Risk Weights			
Risk Factors and Risk Attributes	1	2	3	
4. Employee related				1.51
				Composite Risk Score
	LOW RISK	MEDIUM RISK	HIGH RISK	
Breach of code of conduct	50.00%	50.00%	0.00%	1.5
Acceptance or giving of bribery in the form of gifts or favors	60.00%	40.00%	10.00%	1.7
Insider trading	80.00%	20.00%	0.00%	1.2
Fraud	30.00%	50.00%	20.00%	1.9
5. Outsourced Third Party related				1.58
	LOW RISK	MEDIUM RISK	HIGH RISK	
Complaints against the outsourcing partners/vendors	65.00%	35.00%	0.00%	1.35
Conformance to regulations and standards expected	60.00%	30.00%	10.00%	1.5
Security and privacy issues	90.00%	10.00%	0.00%	1.1
Continuity of services	55.00%	30.00%	15.00%	1.6
6. Customer related				1.39
	LOW RISK	MEDIUM RISK	HIGH RISK	
Not giving or misrepresenting KYC details (Know Your Customer)	60.00%	40.00%	0.00%	1.4
Abuse of financial system	60.00%	30.00%	10.00%	1.5
Money laundering				
Terrorist financing				
Tax evasion				
Misrepresentation of facts	80.00%	20.00%	0.00%	1.2
Improper transactions	30.00%	40.00%	30.00%	2.
				1.53

TABLE 9.15 Example of Compliance Risk Scorecard

Compliance Risk	
Risk Factors and Risk Attributes	
1. Business practices related	**Risk Factor Significance**
Inappropriate Marketing Practices, sales practices (mis-selling)	3.90
Irregularities in Product and Services offered	3.65
Advisory services (improper or misleading)	3.85
Customer complaint management	4.20
New Product Implementation	4.35
2. Organization related	3.99
Market abuse	3.95
Nondisclosures, Incorrect or Incomplete disclosures to all stakeholders including regulators	3.80
Shareholders complaints to regulators	3.70
Negative press for regulatory breaches	3.75
3. Management related	3.80
Breach of code of conduct	3.90
Conflicts of interest in terms of roles within the organization or outside positions held	3.65
New products/services without proper governance structures	3.85
Insider trading	4.20
4. Employee related	3.90
Breach of code of conduct	**4.35**
Acceptance or giving of bribery in the form of gifts and favors	**3.85**
Insider trading	**4.20**
Fraud	**3.95**
5. Outsourced Third Party related	**4.09**
Complaints against the outsourcing partners/vendors	**3.05**
Conformance to regulations and standards expected	**3.15**
Security and privacy issues	**3.20**
Continuity of services	**2.70**
6. Customer related	**3.03**
Not giving or misrepresenting KYC details (Know Your Customer)	**1.30**
Abuse of financial system Money laundering Terrorist financing Tax evasion	**1.20**
Misrepresentation of facts	**2.00**
Improper transactions	**1.10**
	1.40

This is too much detail for management. The summary metrics that are now available (either directly from the previous tables or arithmetically computed) are

- Risk factors
- Risk scores
- Factor significance
- Factor-weighted significance
- Significance-adjusted risk score
- Risk percentage

Table 9.16 captures these summary metrics.

In terms of presentation to the management, the following (both tabular and graphical) may be helpful. Table 9.17 and Figure 9.5 are the risk views before adjusting them with significance of the risk factors.

Inference that can be drawn from Table 9.17 is that compliance risk is the least from the outsourcing part of the business; employee related and business practices, as the top two risk areas, will need the attention of all,

TABLE 9.16 Summary of Compliance Risk Scorecard

Summary View	Risk Score (as in Table 9.14)	Risk Factor Significance (as in Table 9.15)	Weighted Significance (each factor as a component of total significance)	Significance-Adjusted Risk Score	Risk Percentage
Business Practices Related	1.55	3.99	0.20	0.31	30.60
Organization Related	1.53	3.80	0.19	0.29	28.67
Management Related	1.51	3.90	0.19	0.29	29.19
Employee Related	1.58	4.09	0.20	0.32	31.87
Outsourced Third Party Related)	1.39	3.03	0.15	0.21	20.80
Customer Related	1.53	1.40	0.07	0.11	10.56

TABLE 9.17 Unadjusted Risk Score (Tabular)

Summary View (Primary)	Risk Score
Business Practices Related	1.55
Organization Related	1.53
Management Related	1.51
Employee Related	1.58
Outsourced Third Party Related)	1.39
Customer Related	1.53
Overall Risk Score on a Scale of 5	1.51

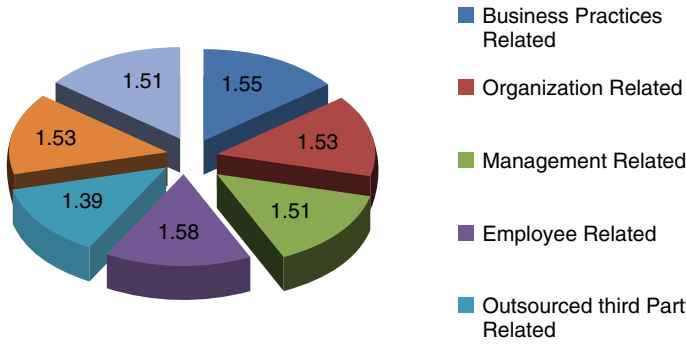

FIGURE 9.5 Unadjusted Risk Score (Graphic)

particularly management, LOB heads, compliance teams, and HR. This analysis is on a stand-alone basis. However, on a relative basis, after weighting it with the significance of the risk factor within the overall landscape, the view could be different based on the significance attached to each risk factor. Figure 9.6 illustrates the significance-adjusted view.

Inference here is that employee and business practices continue to be the top two even after significance adjustment and therefore need to be addressed as top priority. Customer-related is seen as the lowest after adjustment for significance while before the adjustment it was one of the top three risk factors.

How can the significance of customer-related risk factor be low, one might ask. If significance weighting was done based on the control the firm has on managing the risk factor, then of the six factors, four are internal to the firm and two external. Of the two external factors, the firm has a better control on the third-party vendor than on customer behavior. At best it can insist and obtain the mandatory documentation and do KYC risk

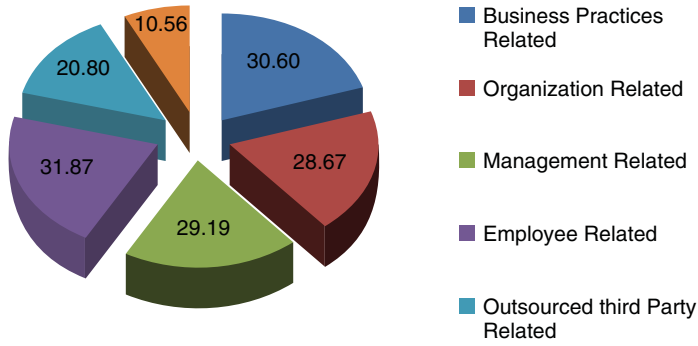

FIGURE 9.6 Risk Score Adjusted for Risk Factor Significance

scoring based on the documentation available and track transaction behavior. Beyond that it is dependent on the customer's integrity to produce genuine and complete information. So the rationale applied here for determining the weights of significance is the extent of control and influence the firm has in managing the risk factors. Is this right, or should the weightage have been the highest, given that financial abuse and crime are what are receiving the maximum fines/penalty, is a valid argument. The illustration here represents the process of building a scorecard methodically. The significance assignment needs to be a well-thought-out and well-debated action.

If a risk appetite statement can be made for compliance risk, banks and financial services firms can potentially state that their appetite both on significance unadjusted or adjusted can be a maximum of 0.25 (it was 1.51 in our example—Table 9.17) at the overall level with individual limits for each of the risk factors. But since compliance risk appetite is not yet considered an option there is generally no stated risk appetite.

This conversation brings out a critical factor of the entire assessment/measurement process. The model and their outputs are dependent on two important factors: the availability and reliability of data on one hand and the soundness and verifiability of the process/logic/outputs of the models on the other. Financial services firms rely heavily on model outputs. If the organizations are not cognizant of the importance of validity of inputs, relevance of the assumptions, the model process (techniques and methodology) applied, and correct interpretation of the outputs might be misled, which could lead to catastrophic outcomes. The regulatory concern and guidelines of model risk management are focused on this aspect, like the Federal Reserve says, "organizations should be attentive to the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused, and should address those consequences through active

model risk management".[4] Models and model risk management is a vast subject by itself. Its relevance here is that the objective of building the models (in this case scorecards), their validity, reliability, maintainability, and usability, have to be kept in perspective and not get lost in the mechanics of it.

RISK MITIGATION

In theory if you have zero risk appetite for compliance risk and can enforce it, then there would be no need for either risk mitigation or monitoring. The fact, however, is that compliance risk is real and the effort to mitigate it on an ongoing basis is a reality. The objective of both risk mitigation and monitoring is to reduce if not totally eliminate the adverse effect/impact of noncompliance.

The first approach, which is particularly true of compliance risk management, is risk avoidance: Taking compliance risk is not worth it and needs to be consciously avoided. In spirit, this is the only approach to follow: Aim for zero risk in compliance risk. It is, without doubt, the most costly option among the risk mitigation options. Note here the "cost" context is not with reference to the consequences of noncompliance but the relative actual costs involved in implementing the various risk mitigation approaches to achieve the "zero risk" state.

While it is a noble objective to pursue, the reality is that there is no such thing as zero risk. The next aspect of risk mitigation is risk acceptance. Risk in its broader context is the cost of staying in business. Compliance risk is the risk of not being in sync with environmental objectives. This deters the organizational objective of value creation and enhancement. The propensity to accept this risk is challenged. In practice, however, risk cannot be eliminated completely; there will always be some element of residual risk. Acceptance of this fact helps firms to be more alert and put in controls to manage them better.

The third strategy for risk mitigation is risk limitation, or risk controls. This is the most common strategy adopted by firms as this, in some form, tries to balance between risk taking and its cost on the one side and manageability on the other. Here there is an acceptance that there would be some risk (inherent risk discussed earlier). As a corollary the expectation is to put in place efficient systems and processes to mitigate it. The objective is to bring

[4]SR 11-7, April 4, 2011, Guidance on Model Risk Management, Board of Governors of the Federal Reserve System.

compliance risk to the absolute minimum that the organization can possibly manage (residual risk). One of the real-life examples discussed earlier is that of total nontolerance of "nonreporting of compliance violations/breaches immediately." This helps limit compliance risk.

The fourth common risk mitigation strategy is risk transference. In compliance risk, however, there is no scope of transference of risk. The firm remains responsible for effective compliance even for outsourced functions and services.

RISK MONITORING

Effective and efficient risk monitoring is at the heart of a successful compliance program. This needs to be both proactive and reactive. It is proactive in terms of capturing a potential breach on time—key risk indicators come in very handy here. Another example could be tracking vulnerable areas based on risk identification heat maps. Reactive risk monitoring is relatively straightforward. The vital thing in risk management is the turnaround time—the key here is the speed to action.

An efficient IT system will be your greatest strength in risk monitoring and mitigation. Automation, alert generation, and action tracking are some of the aspects of a good IT system that assists both in proactive and reactive monitoring. The sophistication of both the processes and systems needs to be in direct proportion to the complexity and geographical spread of the firm.

The compliance plan details the specifics of the responsibility and accountability matrix of the various role holders. It pays to understand these and stay on top of the compliance risk monitoring for areas and functions they are responsible for. Working smart is the only way to manage a voluminous task like compliance monitoring. Prioritizing high-risk items and vulnerabilities and placing them on a more rigorous monitoring cycle are certainly a smart way of managing. Interactive reporting and dashboarding are very important requirements for effective monitoring.

RISK REMEDIATION

Remediation implies the act or process of correcting, reversing, or setting right a deficiency, the prerequisite for which is identification of the deficiency and the impact it is likely to have. I look at redress and remediation at two levels: the internal process improvement idea and the external commitment and requirements of remediation. Together they reduce the snowballing effect of compliance risk. Therefore, it is imperative that there is a policy, process, and dynamic program in place for managing remediation.

Identifying and assessing risk are for an end goal of mitigating risk to acceptable levels based on the risk appetite of the organization. Compliance process improvement is at the heart of internal remediation. Given that there is very low to nil risk appetite for compliance risk, bridging the gap between identification/assessing of risk and reversing or setting right deficiencies in a systematic manner is the responsibility of the remediation process.

From an external perspective the faster, the more transparent, and the more reliable remediation is, the greater the chance of reducing the negative perception of the firm by the stakeholders. This is so because most of the remediation is focused on treating customers fairly and usually in response to enforcement action(s). At an operational and tactical level, there needs to be a remediation standards matrix. These standards are drawn based on the severity and impact scale. Timelines of redress are set against a combination of the two. A word of caution: These timelines are to be set as realistic as possible. Many a time firms have yielded to the temptation to set idealistic standards in their compliance policy statements, found it difficult to abide by them in real situations, and then were rapped on the knuckles by the regulators.

A sample matrix is given in Figure 9.7.

In addition to setting the standards, other aspects of the process like responsibility, accountability, status reporting, tracking to closure, alerting and escalating where relevant need to be clearly laid down. At a strategic level, it is important to identify the root cause and put in place systems and controls to arrest reoccurrence if possible or for early identification (where total elimination is not possible). This learning is to be built into the compliance risk management program.

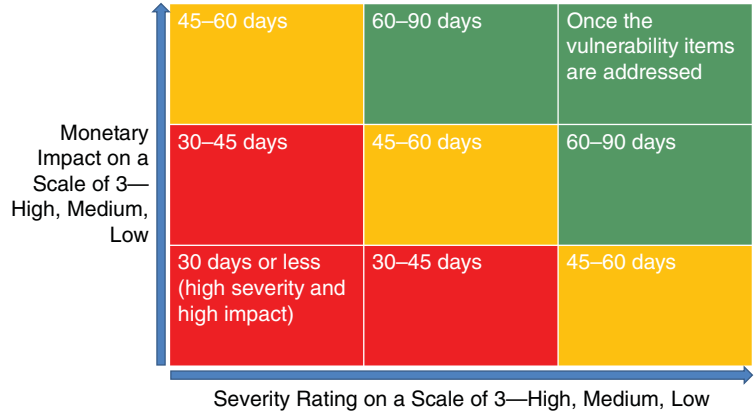

FIGURE 9.7 Remediation Standards Matrix

COMPLIANCE RISK REPORTING

I have said this earlier: In compliance risk management, demonstrating compliance is as vital as actually complying. Firms are invariably challenged on the demonstration part, even more where regulatory compliance is both an expanding and moving target. The surge of rules/regulations from across national, regional, and global bodies and their requirement that they need to "see" compliance will continue unabated. The smartness of the organization is to find opportunities and navigate them while being focused on how to stitch in the new requirements into its dynamic and positive compliance program. This is where a transparent and effective compliance reporting system assumes elemental importance.

Reporting serves two purposes: to demonstrate compliance and to present the status and effectiveness of compliance succinctly. The former primarily serves external stakeholders and the second the internal audience. It helps management make informed decisions.

The trick in designing reports, other than the regulatory reports, which come with predesigned templates, is to keep it simple and intuitive, especially to senior and top management. The heat maps used in the compliance world serve the purpose well as long as the underlying constructs are logical and verifiable. The other aspect that needs to be kept in perspective is ensuring that there is a uniform understanding of the reporting/dashboarding language. This holds true whether it is a five-scale assessment or a three-scale assessment. The terms "critical," "high," and "medium" need to be understood similarly by all levels of the firm both in terms of meaning and impact.

The fundamental edifice of a report is dependent on two critical components—the design of the report and the underlying data—both of which determine the quality, usability, and credibility of any report. Multiple data marts and multiple reporting templates, in addition to being costly, risky, and maintenance heavy, also are counterproductive in the context of a dynamic compliance-reporting universe.

Reports are for the consumers, the audience who needs to act on the report, not the report generator, who understands the context and content from data up. This is where the design of the report becomes vital. The slicing and layering of reports in a way that is meaningful for the level of employees of the firm to whom the report is being presented is critical for the success of the firm. This is not to say that different reports have to be built for different audiences. The idea is to organize data at as granular a level as possible, building in aggregation flexibility. This will enable different groups to see different slices of the *same* data at different levels of detail and aggregation, which then lends itself to drill through to access detail if the audience so desires (Figure 9.8).

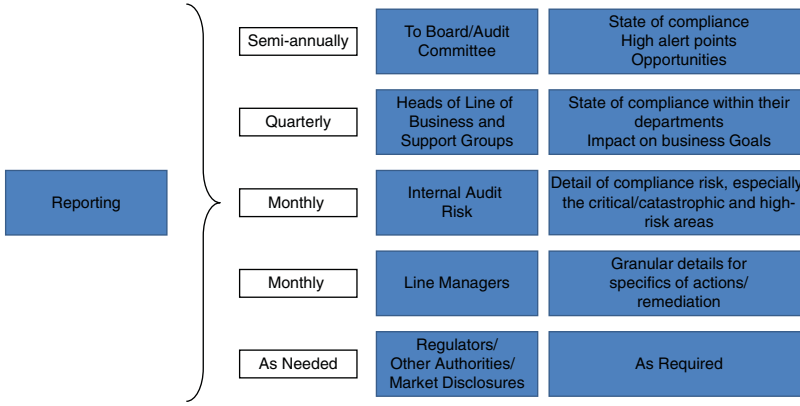

FIGURE 9.8 Reporting Levels and Possible Content

REGULATORY DIALOGUE

Regulatory dialogue is one of the most critical components of compliance risk management, as we have mentioned in Chapters 6 and 7 and will detail further in Chapter 12. In a shifting landscape with a well-meaning but intrusive and aggressive regulatory regime (here again the term *regulatory* encompasses all external authorities that supervise compliance) and the all-pervasive media, it is imperative that a relationship based on trust is built with the regulators. The starting point is to remember that regulators are co-owners of the responsibility of creating a facilitative compliance environment. Verifiable, data-based, and objective conversation is the professional way that will help to positively navigate the regulatory dialogue. The risk of misinterpretation is the biggest risk for both sides, and it is in the interest of the financial firm to ensure that they are on the same page with the regulator in terms of the interpretation of expectations from the firm and also that they present actual compliance in a way that it is clear to the authority.

Reaching a common understanding and an ABC analysis of what is required is a good start. The reason I say "ABC analysis" is to bring reality into the conversation. Theoretically speaking, all requirements need to be fulfilled across the compliance spectrum, but in reality the dialogue is usually centered on some vital aspects. Some examples could be the stress testing results, corporate governance high-alert points, financial crime indicators, fair treatment of customer related, new products and services introduced, and remunerations and incentives.

We have spoken earlier in the book of how regulators make a distinction between willful default and an unintentional miss. They factor past compliance history while awarding strictures/penalties. It is not uncommon that for the same offense two organizations may be awarded different levels of strictures/fines/penalties based on their perception of the sincerity of the firm in implementing compliance in letter and spirit. Open and ongoing communication fosters an element of trust with this very important stakeholder. Firms that have an open and trust-based relationship with the regulators are the ones best equipped with managing the ever-changing landscape of regulations.

The ultimate responsibility of managing regulatory trust typically rests with the CCO, CXO, or a subcommittee of the board. There will also be dialogue at other levels of management/compliance role holders. Consistent messaging across all levels is critical to the success of this process.