Becoming ‘Reactively Proactive’ Rethinking compliance risk management in today's environment

J.H. Caldwell
Partner
Regulatory &
Risk Strategies
Deloitte US

John Graetz
Principal
Governance, Regulatory
& Risk Strategies
Deloitte US

Thomas Nicolosi
Principal
Enterprise Risk Services
Deloitte US

Susan Jackson Redman
Senior Manager
Enterprise Risk Services
Deloitte US

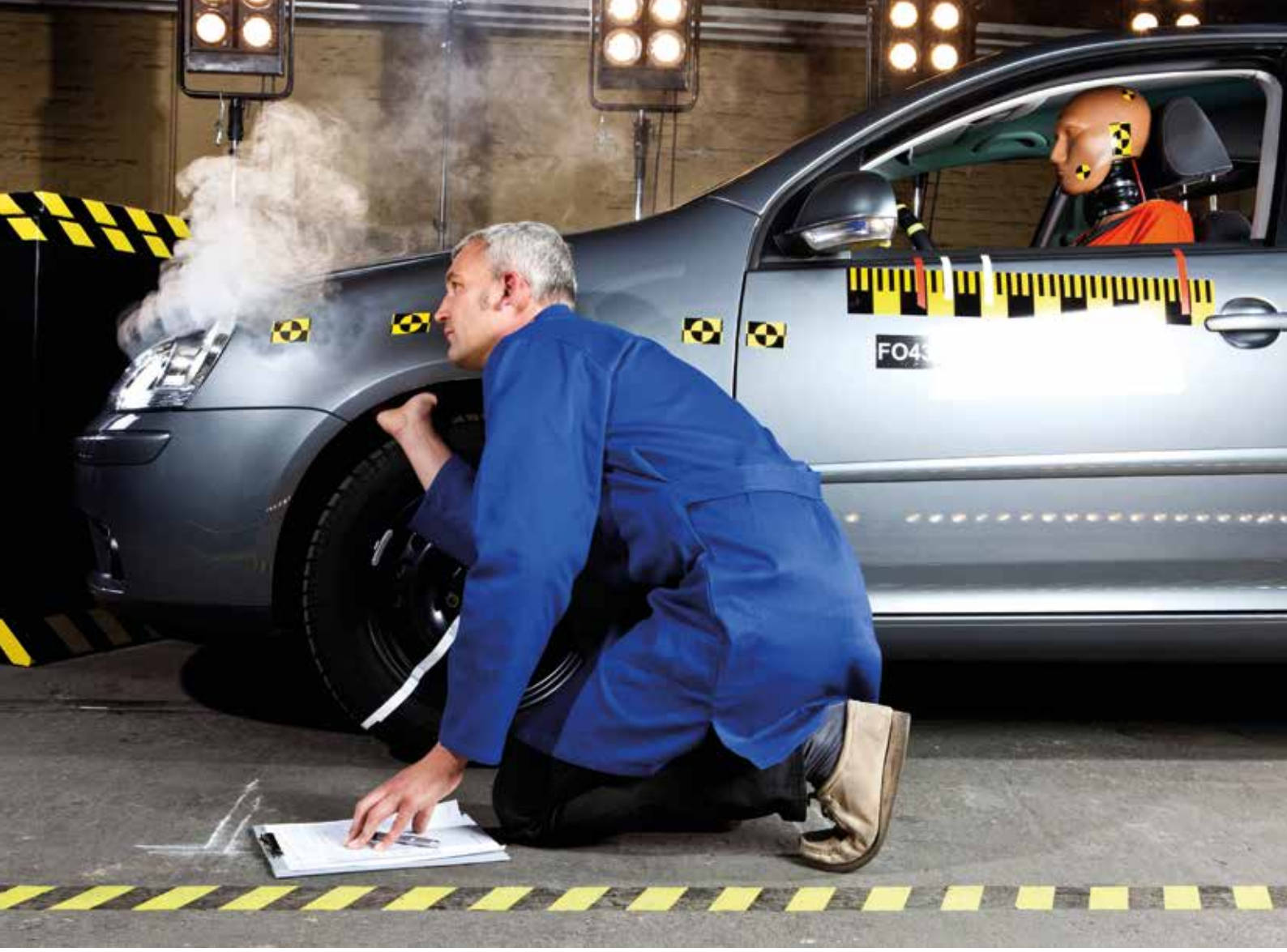
Anna Blythe Papson
Manager
Enterprise Risk Services
Deloitte US

Joanna Connor
Senior Manager
Enterprise Risk Services
Deloitte US

Introduction

In light of recent and ongoing changes in the global financial markets, there is a significantly increased focus on the supervision and regulation of the financial services industry. Changes in existing laws, rules and regulations, together with new requirements and regulatory expectations, are likely to have a material effect on a financial institution’s operating model.

The global regulatory environment has been and continues to be fluid and increasingly complex as a result of regulatory reform. Financial institutions are faced with a number of new regulatory obligations, tougher restrictions on risk taking, greater day-to-day direction by regulators, increased scrutiny of reliance on third parties and increased costs for compliance.



The regulatory changes are largely the result of the following factors:

- **Supervision:** The new environment is more prescriptive, less flexible and less predictable
- **Legislation and regulation:** The regulators are focused on reducing risk through the enhanced prudential standards, an orderly resolution scheme and greater consumer protections
- **Focus on operational processes that give rise to regulatory risks:** Regulators have clearly stated an expectation for increased oversight of operational risks, particularly where operational failures increase compliance risk and impact consumers
- **Enforcement:** The regulatory culture has become more enforcement driven as a result of the financial crisis, including enforcement surrounding consumer and trading related activities
- **Global regulatory coordination:** Regulators are collaborating more across borders to ensure that they have a comprehensive supervision strategy

This environment is creating a new challenge for the executive management and boards of financial institutions, which must come to terms with the new reality of compliance. What is the size and shape of the compliance infrastructure (e.g. people, process, and technology) they need to have in place to remain compliant – and avoid the major fines and reputational risks that come with enforcement?

Is the entire organisation acting in a consistent and strong manner when it comes to compliance? These are the types of questions many financial institutions have been wrestling with recently. As a result, the outlines of a new compliance framework have begun to emerge and take shape. In this article, we will describe some of the many important tools and considerations being used by industry leaders as they respond to more stringent and forceful regulatory scrutiny.

Find your baseline: strategic self-assessment

A starting point for a financial institution in determining its compliance with all laws, rules, regulations and regulatory guidance is to perform a strategic self-assessment of the overall compliance risk management programme in light of the new global regulatory environment. For many organisations, this is a common technique used today; however, few have actually undertaken the effort required to proactively assess their level of compliance with regulatory guidance, largely because 'knowing' has not been mission-critical. Today, what you do not know may hurt your organisation and many financial institutions find themselves becoming reactively proactive to stay ahead of the regulators.

Several whitepapers from the Basel Committee on Banking Supervision (BCBS), including *Compliance and the Compliance Function in Banks (BCBS 113, April 2005), Principles for Sound Management of Operational Risk (BCBS 195, June 2011)* and *Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239, January 2013)* as well as resulting guidance by various home country regulatory agencies have arguably evolved certain regulatory principles into outright requirements. As a result, many financial institutions have implemented compliance risk management frameworks to address them. However, many financial institutions' execution of these frameworks has been viewed by the regulators as being inadequate in meeting the heightened regulatory standards.

The shortfalls often involve weaknesses in establishing independence for compliance management and staff and decisions around the adequacy of the compliance budget, compensation for personnel, performance evaluations, compliance testing, training, policies, procedures and effective escalation of compliance issues. These can impact the financial institution's ability to effectively aggregate, analyse, report and holistically address compliance issues across the enterprise.

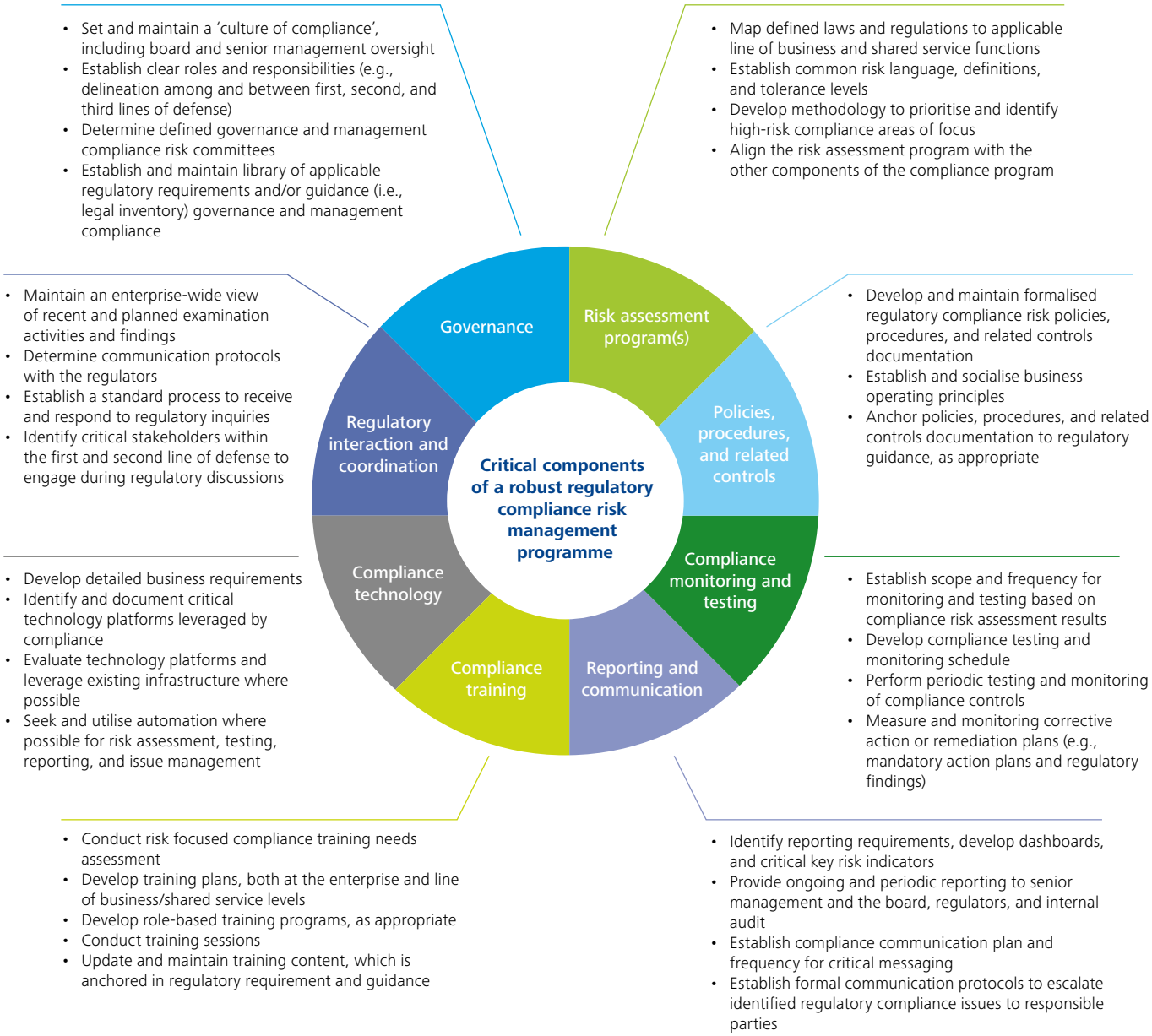
Strategic self-assessments can be important tools for identifying and assessing how compliance risks are being overseen at both the line-of-business and enterprise levels. In addition, they can be critical in helping organisations prepare for internal audit and regulatory examinations by assisting in proactively identifying issues and non-compliance and allowing for time to address such issues prior to examination start dates. When performing a self-assessment, it is prudent to anchor regulatory guidance to business/enterprise controls and processes, which helps to provide additional insight and transparency of where requirements are being met (or where they are lacking) within an organisation.

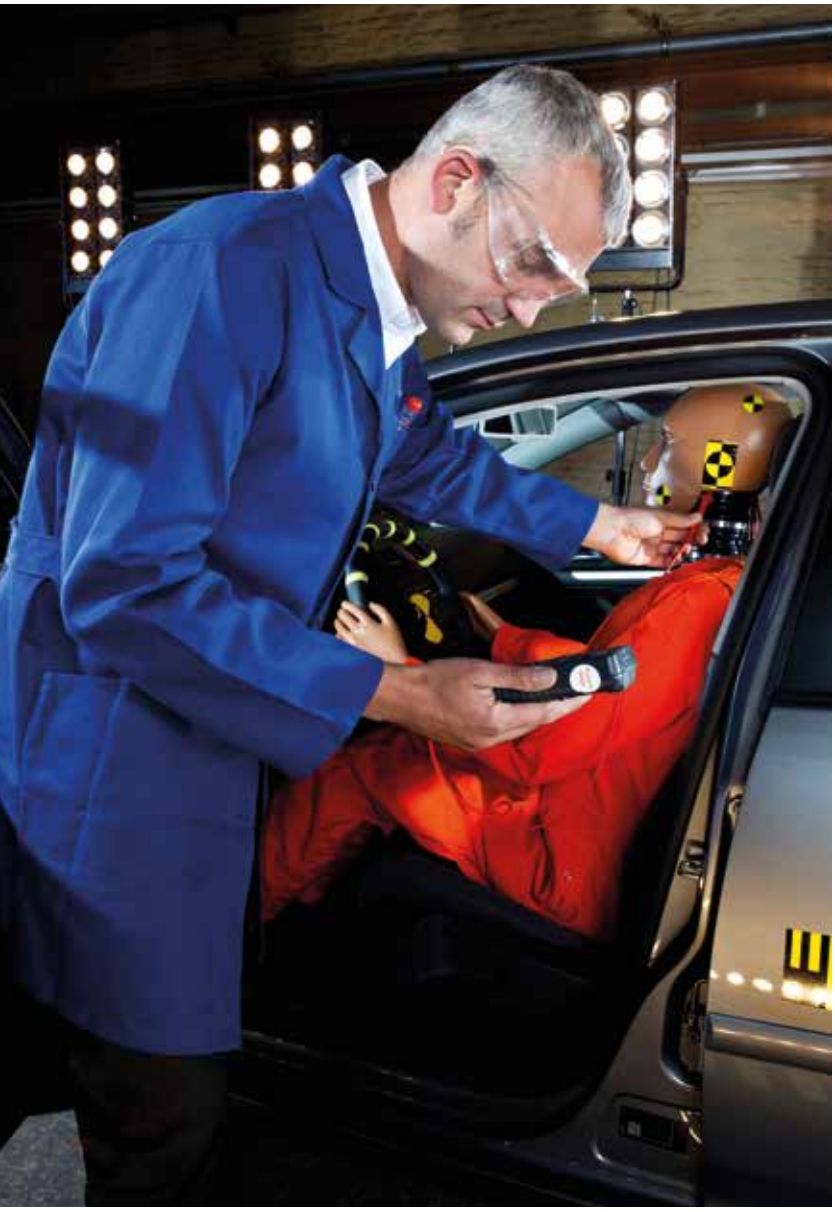
The self-assessment may be used as a basis for analysing certain aspects that are key components for a compliance program framework (see *Figure 1*). These key components include governance, risk assessment programme and controls, policies and standards, compliance monitoring and testing, reporting and communication, compliance training, compliance technology as well as regulatory interaction and coordination. With respect to these components, there appear to be emerging and common industry challenges towards designing and executing effective compliance programmes.

These challenges underscore the focus of the BCBS 113 compliance principles and include among others:

- A firm-wide approach to compliance risk management that generates meaningful compliance risk information and analysis capabilities, not just static reporting
- Formalised and systematic processes and clear responsibilities and accountabilities to support independent compliance oversight
- Comprehensive and risk-focused compliance monitoring and testing that evaluates control effectiveness as well as compliance with laws and regulations
- Analysis and reporting tools to facilitate effective board and senior management oversight

Figure 1: Critical components of a robust regulatory compliance risk management programme





Make the map: Strategic planning

Once an organisation has determined its baseline and identified any compliance programme gaps, the next step is to build a strategic plan. Banks have no shortage of strategic plans in place, but when it comes to compliance, there is often comparative radio silence. For many, that is largely due to the fact that the compliance function is viewed as less important than a growth-oriented, profit-driven line of business. To quote Susan Bies, former U.S. Federal Reserve Board governor and now board member for a top-tier U.S. financial institution, *'A culture of compliance should establish—from the top of the organization—the proper ethical tone that will govern the conduct of business. In many instances, senior management must move from thinking about compliance chiefly as a cost center to considering the benefits of compliance in protecting against legal and reputational risks that can have an impact on the bottom line.'*[1]

In reality, the cost center-view of compliance is quickly becoming outdated as compliance becomes increasingly enmeshed with core business strategy.
It is hard to imagine accomplishing any strategic goal without incorporating regulatory compliance. In fact, a strong compliance function can help an organisation gain competitive advantage by mitigating legal and reputational risks and further unlocking value through efficient and effective risk management. So after taking the important step of self-assessment, there is another fundamental question to answer: How do we take the assessment of our current state of compliance and leverage that information to build our future-state vision and goals? Building an in-depth strategic plan is the next critical step.

The strategic plan for compliance is a formalised vision and strategy for the compliance function – one that answers familiar strategy-level questions such as:

- What does our compliance function seek to achieve?
- What is the mission and vision of compliance?
- How will compliance support core business goals?
- Is there an opportunity to drive further cost efficiency through the use of technology and tools?

It is also important to remember that this is a strategic plan only for compliance risk, not risk management overall. An organisation may already have a strategic vision for risk management. But compliance risk is so important today that it warrants its own compliance-specific strategic plan with the overall vision of the organisation considered in the context of compliance-specific development needs.

In addition to providing the organisation with significantly increased clarity on the desired role of the compliance function, such a plan can be a useful tool in communicating with regulators. Regulators recognise that to maintain or become compliant in a radically changed environment is a challenging proposition that will not happen overnight with the waving of the proverbial magic wand. Besides the fundamental core day-to-day compliance activities, regulators also want to know that an organisation has a plan for getting there – along with the board and executive team. The strategic plan certainly may help.

1 *Bies, Susan Schmidt, 'Enterprise-Wide Compliance Programs,' Remarks at the Bond Market Association's Legal and Compliance Conference, New York, NY, February 4, 2004. http://www.federalreserve.gov/boarddocs/speeches/2004/20040204/default.htm*

All about execution: The action plan

Once the strategic plan has been built, detailed actions and milestones for executing the plan should be defined and documented via an in-depth action plan. The action plan should address gaps identified during the self- assessment process, actions required for implementation of the strategic plan and any open regulatory findings pertaining to the financial institution's management of compliance.

Associated target completion dates for each action should be identified. These dates should be heavily considered and discussed prior to being documented, as it is likely that the action plan will be shared with internal audit and the regulators and dates will be socialised, especially if there are any open regulatory findings related to any actions.

In addition, specific executives should be made accountable for each action. Demonstration of executive accountability and tone at the top is key in satisfying regulatory expectations and, perhaps even more importantly, when organisational transformation is underway to win the support of financial institution's associates. It is critical that associates experience the commitment to change, as their willingness to play an integral part in the operationalisation of the financial institution's strategic plan and target operating model is vital for the success of the future-state vision.

Effective execution of the action plan will typically lead to the revision of various elements of the enterprise compliance programme such as governance, compliance risk management committees, global compliance policy and procedures, risk assessment process and monitoring as well as testing methodology and plans.

This will not happen overnight

It takes time to move the needle on compliance in a new environment like the one financial institutions face today. There are new policies and procedures to be developed and implemented, process and technology impacts to address across the organisation. Nevertheless, the only way to gain momentum is to begin making some moves, no matter how small. In this case, the place to start is with the self-assessment. Just remember that the assessment is an important commitment that will undoubtedly uncover important gaps to be addressed.

Many could say that this exercise is not just a nicety. A new approach to managing compliance risk is necessary and is now a more-important-than-ever component of a growth plan.

What a typical strategic plan should look like

While there is no official view on what a strategic plan should look like, the content listed below offers a good guide as to what key components should be considered. As you can see, the intent of the plan is to go well beyond a gap analysis. It should be a practical, strategic guide to compliance risk management.

- Executive summary
- Mission statement
- Vision statement
- Global regulatory environment
- Current-state observations
- Future-state vision