The Benefit of Adopting a Management System Approach to Regulatory Compliance

Author: Jeff Fieldhouse, Principal Consultant, Baines Simmons

This paper has been developed to challenge a traditional reactive approach to meeting regulatory compliance requirements. It explains why Baines Simmons advises approved organisations to adopt a management system approach that is fully aligned with the intent of the regulation and integrated with commercial management processes. This approach allows organisations to demonstrate compliance, whilst gaining increased stakeholder confidence and significant business advantage.

Introduction

Aviation regulations have evolved in response to a long history of accidents and failures. Compliance is often seen as a ‘bolt on’ or as ‘something organisations have to do’ and many organisations still perceive compliance as a distraction, blindly missing the opportunity to learn from the mistakes of others. Frequently, regulatory compliance only takes centre stage when there has been an audit finding or a significant impact on the operation, where potential losses are real and tangible.

The intent of regulation is predominantly focussed upon the prevention of harm¹ and the fundamental aim is to require organisations to develop systems that drive a safe and efficient operation. Integrating regulatory compliance within the organisation’s management system has many safety and commercial benefits that can only be realised when they understand the intent of the regulation. In a military context, business output or benefits, relate to the optimised availability and use of aviation assets and the effective control of costs. This paper does not differentiate between the two sectors as the principles are entirely aligned.

¹ Protection against loss of life or injury as well as loss of reputation, customers, assets, regulatory approval, etc
With the introduction of Performance-Based Oversight (PBO), the regulation is moving away from binary ‘yes’ or ‘no’ requirements towards a more objective-based set of guidelines. This regulatory evolution is designed to deliver significant safety and business benefits. It focuses on the implementation of a management system that, if truly effective, appropriate and adequate against the intent of the regulation, will create opportunity to drive focus on the delivery of the desired business output, whilst still complying with the rules. However, this new approach presents a number of challenges. Organisations that do not fully understand the intent of regulation are unable to build effective and integrated management systems. This is even more challenging in a complex organisation with multiple approvals.

It is our experience that many senior executives do not appreciate how regulatory compliance can benefit business performance and therefore how it can be a key management aid. Regulatory compliance is often an isolated activity that is not integrated with the rest of the business but instead focuses on reactively trying to keep the regulator satisfied. However, by embedding compliance controls into an organisation’s core business management systems, senior leaders can secure increased confidence that compliance is being proactively managed within day-to-day activities. This, in turn, frees them up to stay focused on strategic management challenges. This proactive approach to regulatory compliance will result in a reduction in harm, improved efficiency and confidence that safety risks are being appropriately managed.

The evolution of the regulatory landscape

Regulations in aviation have been evolving for almost one hundred years. It started with the Paris Convention of 1919, which was the first global initiative to regulate aerial navigation. The biggest influence came from the setting up of the body we now know as ICAO (International Civil Aviation Organisation), which was born at the Chicago Convention on 7th December 1944. The primary objective of ICAO was to develop international civil aviation “in a safe and orderly manner.”

Since 1944 regulation has continued to evolve outside of the technical mechanisms of aircraft, taking a deeper focus into the human and system interaction and interfaces (see Figure 1)
The introduction of many new and completely valid regulatory initiatives has invited Organisations and Regulators to take a spotlight approach to compliance (Figure 2). The intent was always to promote progressive advancement through the introduction of each initiative, and to consolidate and integrate these fully, before moving on to the next. In reality, many organisations have not fully adopted this approach, therefore compliance, safety management and business management systems operate in silos, creating a disjointed approach where systems do not integrate. To become truly effective, organisations must move away from the spotlight approach towards developing an integrated management system that embraces them all.

Who owns regulatory compliance?

This is a simple question which should prompt a simple answer. However, many approved organisations still believe that compliance responsibility sits with ‘Quality’, ‘Compliance Monitoring’ or even ‘the Regulator’. For those organisations, the ownership of regulatory compliance is still unclear, therefore suggesting that compliance may not be managed as effectively as it could be. A lack of accountability and ownership can only be negative – increasing risk, damaging business performance and reducing stakeholder confidence.

Compliance is defined as, ‘the act or process of doing what you have been asked or ordered to do’. Therefore if compliance is the act of doing then arguably this rules out the responsibility of quality and compliance monitoring departments. This is because it’s their role is to monitor. Furthermore organisations should by no means expect the regulator to ‘do’ compliance on its behalf. Crucially, compliance must be owned by those who have been identified by the organisation to ensure it ‘remains in compliance’ e.g. Nominated Persons.

---

Figure 2: Key Regulatory Initiatives and the Spotlight Approach

http://www.merriam-webster.com/dictionary/compliance
If we consider the following ORO\(^3\) requirements it clearly states who should own and who should monitor compliance:

- ORO.GEN.210: “A person or group of persons shall be nominated by the operator, with the responsibility of ensuring that the operator remains in compliance with the applicable requirements.” - Compliance owner
- AMC1 ORO.GEN.200(a)(6): “The role of the compliance monitoring manager is to ensure that the activities of the operator are monitored for compliance with the applicable regulatory requirements” - Compliance monitor

Whilst the regulation is eloquent in its portrayal of ownership requirements, it is still very much misinterpreted or misunderstood and disconnected from business benefits. Quality or compliance monitoring functions are being burdened with the responsibility for owning compliance, and in so doing are not fulfilling the intent of the regulation. This misinterpretation is costly and fundamentally erodes confidence in an organisation’s safety protection system.

**A management system approach based on the ‘three lines of defence’ model**

The Regulator is now influencing Organisations to take a management system approach to compliance. A recently published EASA Opinion on the introduction of SMS into Part M specifically states as one of its objectives:

- Opinion 2006/06\(^4\): ‘That the proposed changes are expected to facilitate the implementation of single management systems by multiple-approved organisations and streamline the related oversight’

The Opinion further elaborates and demonstrates organisational benefits by stating:

- Opinion 2006/06: ‘A Safety Management System is something implemented not solely to prevent incidents and accidents but to ensure the success of as many elements of an organisation’s business as possible, any investment in safety should be seen as an investment in productivity and organisational success’

The Three Lines of Defence model supports the integrated management system approach and can also be used as the primary means to clarify and present roles, responsibilities and accountabilities for decision-making and effective compliance.

The model is a risk governance framework that is extensively applied within the financial services sector and is the recognised best practice approach to managing and controlling corporate risk\(^5\). It is equally compelling when transposed to an aviation context as it provides a robust framework for managing compliance.

---

\(^1\) EASA - Commission Regulation (EU) No 965/2012 - Organisation Requirements for Air Operations

\(^2\) Embodiment of safety management system (SMS) requirements into Commission Regulation (EU) No 1321/2014 - SMS in Part-M

\(^3\) IIA Policy Paper, Chartered Institute of Internal Auditors
A policy paper published by The Institute of Internal Auditors (IIA) sets out a Three Lines of Defence approach that provides clarity on how ‘different parts and levels of an organisation play different roles in risk management, and the interplay between them determines how effective the organisation as a whole is in dealing with risk’. The IIA describe the Three Lines of Defence as:

1. **First line of defence** - functions that own and manage risks

2. **Second line of defence** - functions that oversee or who specialise in compliance or the management of risk

3. **Third line of defence** - functions that provide independent assurance

*Figure 3: The Lines of Defence Applied to Aviation Compliance*
Applying ‘three lines of defence’ to regulatory compliance

In applying this model for the aviation context ‘risk’ is exchanged for ‘compliance’. This provides the foundation of a regulatory compliance management system. On the understanding that safety regulations have been formed through learning from past incidents and therefore they form the minimum standardised aviation safety risk mitigations required by the Regulators, then it should be recognised that management of compliance and risk are one and the same.

**First line of defence** - Those that own and manage compliance through day to day functions and system/quality controls

The first line of defence is the act of doing compliance, which is owned and delegated by Nominated Persons. For the first line of defence to be effective it requires managers to possess a complete understanding of the relevant compliance framework(s). This is so that the organisational structure can be aligned with the needs of the operation and that processes and standards accurately reflect compliance requirements within everyday activities. It is the role and responsibility of the Nominated Persons to ensure that compliance is managed and that early warning signs of non-compliance are provided and acted upon.

**Second line of defence** - Compliance owners demonstrating compliance control (Measurement and Reporting)

The second line of defence is the act of managing the doing of compliance and owned solely by Nominated Persons. The second line of defence requires a method of accurate measurement and reporting, that provides a first layer of confidence to stakeholders that compliance is being managed and controlled. Nominated Persons are also responsible for setting direction, giving guidance and the implementation of compliance activities. It is important to recognise that compliance is not managed by ‘Quality’ or Compliance Monitoring functions.

In other words, the first two lines of defence can be summarised as O.D.D. - Ownership, Delegation and Demonstration. These are the cornerstone principles for ensuring compliance in your organisation.

**Third line of defence** - Compliance monitoring (Independent assurance – QA/CM)

The third line of defence is the act of assuring the doing and is managed by an independent assurance function (Quality and Compliance Monitoring (CM)). Independent assurance provides key stakeholders with the confidence that regulatory compliance is being managed effectively. It is a gatekeeper and value-adding function that captures any drift in the compliance management system so that the organisation can learn and continuously improve.

For the third line of defence to be effective a comprehensive assurance programme is required and then delivered by competent auditors. This independent assurance function provides confidence to the relevant stakeholders that all the applicable requirements of the organisation’s compliance framework are being met. A key responsibility of the Quality and Compliance Monitoring functions is to deliver effective feedback from the assurance programme. Feedback is given to the relevant Nominated

---

6 A compliance framework is the complete scope of work deemed to constitute the approvals an organisation holds, and demonstrates how the organisation intends to comply with the regulations including contracting and supplier obligations

7 Such as the Accountable Manager, the Regulator, board of Executives and clients, investors etc.
Persons so that system improvements can be established, implemented and maintained. Quality and Compliance Monitoring Managers are also responsible for ensuring that the assurance programme is properly implemented, maintained, continuously reviewed and improved.

**Conclusion**

Mistakenly, many organisations still see compliance as an overhead or a bolt-on, however the bottom-line is that approved organisations will not be able to operate at all if they lose their regulatory approval. It is therefore necessary to ensure that regulatory compliance attracts a higher profile and that compliance requirements are embedded within ‘business as usual’ activities. This will result in a reduction in harm, improved efficiency and increased confidence that safety and thus business risks are being appropriately managed.

Adopting a management system approach, using the Three Lines of Defence model, will ensure that organisations understand the value of compliance and no longer view it as ‘bolt on’ or as ‘something they have to do’. When implemented in an aviation context, the Three Lines of Defence model can be used as a way of understanding and communicating the roles and responsibilities required to support compliance management, robust assurance, and ultimately business performance.
About the Author

Jeff Fieldhouse
Principal Consultant, Baines Simmons

Jeff is a highly proven specialist consultant in delivering and leading projects in aviation quality, safety and regulatory safety performance improvements. He uses his deep understanding of the continued airworthiness regulatory requirements and auditor and investigation expertise to effectively enhance organisational safety cultures. He leads and manages a team of highly qualified consultants across civil and defence client organisations.

Career background and experience:

A licensed engineer, Jeff has broad experience in aviation, with a particular focus on quality, being qualified in Quality Assurance and as a lead auditor. Jeff is a member of the Chartered Management Institute and has a Chartered Management diploma. Jeff’s experience includes working for 16 years at British Airways, responsible for auditing and maintaining company standards including liaison/review of current/new EASA, FAA and CAA legislation and creation and delivery of an effective and sustainable MEMS programme.

About Baines Simmons

We are specialists in aviation regulations, compliance and safety management and partner with the world’s leading civil and defence aviation organisations to improve safety performance.

As trusted advisors to businesses, armed forces, governments and regulators across all sectors of aviation, we help to advance best practice, shape safety thinking and drive continuous improvement to safety performance through our consulting, training and outsourced services.