FSPCOMP5: Communicate and implement your compliance policy within your organisation

PraxisGRC: Communicating Compliance and NOS COMP5

Focussing on FSPCOMP5

FSPCOMP5 is one of a suite of competency standards developed for financial services compliance professionals. The value of these NOS, however, stretches far beyond financial services and has formed a key part of training offered to GRC professionals across many industries and sectors.

COMP5 "is about effectively communicating and implementing your [organisation's] compliance policy… [that is] underpinned by an implementation plan which is realistic and achievable, and [compliance practitioners] must help the people involved, specifically senior management and the board, to understand and support it. [GRC practitioners] must consider ways in which the policy can be communicated which will set out the vision and values for compliance within [their] organisation".

FSPCOMP5: performance criteria

Each NOS competency unit contains, as a minimum, a list of performance criteria (what a practitioner must be able to do) and knowledge and understanding (what a practitioner needs to know and understand.

Criteria for COMP5

Practitioners must be able to:

1. develop an implementation plan for the compliance policy that includes the business benefits by reference to factual evidence
2. promote the benefits and importance of the policy to senior management and the board in a way that encourages constructive debate, facilitates decision making and secures organisational commitment
3. outline the business implications of introducing the compliance policy, inviting staff to ask questions and provide feedback
4. confirm that the regulatory responsibilities regarding the policy are understood, and provide support where this is not the case

FSPCOMP5: performance criteria (continued).

Criteria for COMP5

Practitioners must be able to:

5. identify approaches to the education, training and awareness-maintenance of the compliance policy to all staff
6. explain the benefits of compliance policy with reference to examples of good practice within the organisation
7. communicate the policy across the organisation
8. ensure that staff have a clear understanding of the regulations that apply to them and their work, and the importance of complying with them

FSPCOMP5: knowledge and understanding criteria

Each NOS competency unit contains, as a minimum, a list of performance criteria (what a practitioner must be able to do) and knowledge and understanding (what a practitioner needs to know and understand.

Criteria for COMP5.

Practitioners need to know and understand the:

1. need for and benefits of stakeholder engagement for the implementation of the compliance policy
2. legislation and regulations that apply to [the] organisation
3. importance of consulting with colleagues and management during the development of strategic/ operational plans and how to do so effectively
4. different methods of communicating the policy effectively across the organisation
5. different methods of encouraging engagement and feedback with the policy
6. why it is important to support staff in their responsibilities within the compliance policy
7. measures and methods which can be used for monitoring and evaluating performance
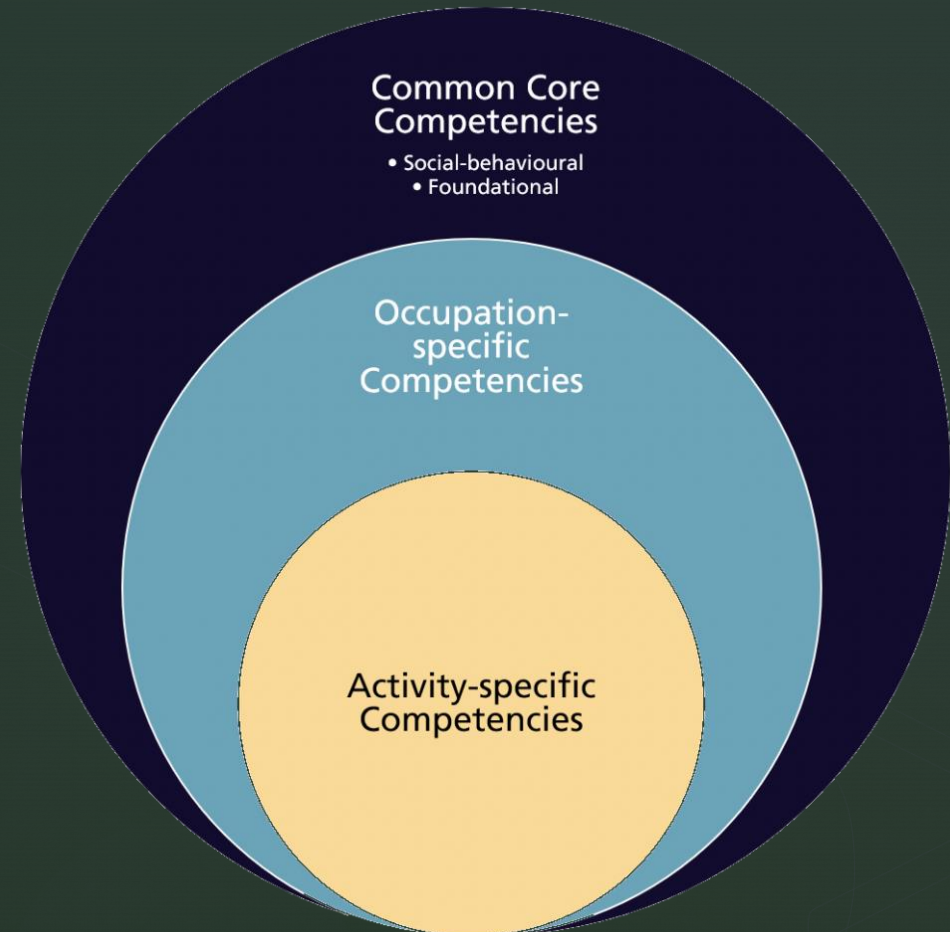8. where to find information that can aid monitoring and evaluation

Implications of COMP5

The main implications are that the basis for effective compliance communications, the knowledge, understanding and performance criteria, are described in practical ways that allow a broad range of uses within an organisation. For example:

- conducting a compliance training needs analysis for the organisation and, on that basis, establish how well compliance is understood by stakeholders

- identifying the organisation's concepts of responsibility and accountability for compliance matters

- establish the level of engagement with codes of conduct

- instigate or further develop HR tools such as performance reviews, target setting and the broad range of monitoring, for alignment of individuals behaviours with compliance and risk management

- review the traction that transparent and observable actions (e.g. through bulletins) from top management relevant to organisational strategic compliance objectives

- ensure risks and opportunities for compliance purposes are captured, analysed, evaluated and that reporting and monitoring focuses on business conduct and people risks more generally

- that corporate structures steer compliance competence, enable cooperation and collaboration where appropriate, and facilitate autonomous and independent actions and decisions within the scope of relevant policy and procedures.

Performance Criteria

1. Set performance standards and goals
2. Measure performance
3. Compare actual performance to established performance standards
4. Take corrective action
5. Use information gained from the process to set up future performance standards

Common Core Competencies
- Social-behavioural
- Foundational

Occupation-specific Competencies

Activity-specific Competencies

Performance criteria #1

Practitioners must be able to develop an implementation plan for the compliance policy that includes the business benefits by reference to factual evidence

The compliance policy will broadly establish: your organisation's approach to compliance; define the management framework; specify regulatory compliance topics; set operational guidelines for functions/ departments/ teams; reference management standards and codes of conduct, which includes specific guidelines for staff engaged in compliance activities.

The policy should capture all relevant prohibitions from civil and criminal law and regulation, reference external and detail internal regulations: compliance policies allow employees to understand behavioural norms and boundaries without needing to consult jurisdictional laws and regulations.

Implementation planning includes, as a minimum: the compliance risk management system and the controls framework, a compliance monitoring programme, as well as mechanisms to respond to non-compliant activities, products and services.

One significant part of the implementation to consider is communication planning, which includes guidance, bulletins, direct advice, as well as training interventions.

Performance criteria #2

Practitioners must be able to promote the benefits and importance of the policy to senior management and the board in a way that encourages constructive debate, facilitates decision making and secures organisational commitment

Making management one of the cornerstones of the compliance policy communication strategy. means senior management, including the CEO, should communicate directly with employees about ethics, integrity and compliance risks, while remaining open to hearing concerns or resolving problems. Gaining the understanding of top management and senior managers is, therefore, vital.

It is essential to communicate the compliance policy in a way that interest is both generated and retained: proactive measurement of compliant and non-compliant outcomes, alongside root-cause analysis of matters of concern, can establish the extent to which compliance is known and understood by top management and staff at all levels.

Adopting strategies to communicate with digitally connected remote workers, as well as creating bespoke micro-learnings and briefings, are more likely to gain traction for the Compliance function in promoting the organisation's compliance policy. The facility of a digital rule book enabling push notifications to individual staff members' Smart phones helps board, senior managers and staff to be kept up-to-date about the achievement of compliance engagement.

Performance criteria #3

Practitioners must be able to outline the business implications of introducing the compliance policy, inviting staff to ask questions and provide feedback

Explaining what regulatory risks and vulnerabilities an organisation faces is an essential role for compliance practitioners. An up-to-date compliance policy will contain the latest information on the legal and regulatory environment, the associated supervisory regime, and the duties and obligations of the business. It will also indicate the serious consequences of non-compliance.

Important business implications include:
• building and supporting a positive reputation, creating trust from all stakeholders
• improving and maintaining employee's morale, by securing confidence in management
• ensuring transparent processes, which encourages and supports accountability
• delivers effective regulatory and wider risk mitigation
• establishes a culture of integrity and facilitates the development of business maturity, resilience and sustainability.

Compliance practitioners will be able to provide an overview of the existing state of compliance within their organisation, highlighting strengths, vulnerabilities and the need for improvement.

Performance criteria #4

Practitioners must be able to confirm that the regulatory responsibilities regarding the policy are understood, and provide support where this is not the case

One significant aspect of a compliance practitioner's work is their role as advisors, consultants and guides to senior leaders and staff working in the first line of defence and other risk-facing positions. It is not the role of the practitioner to shoulder others' responsibilities, but they should be able to alleviate some of the concerns staff have about meeting their duties, obligations and responsibilities for compliance.

This requirement goes beyond communications plans and strategies and involves building strong relationships throughout your organisation, as well as developing a strong commercial understanding so that the compliance practitioner can properly empathise with the situations and pressures faced by individuals in their organisation. Important communication skills, in this respect, is learning to actively listen, engage in and respond appropriately to discussions, and to develop a strong sense of mutual respect and confidence.

Performance criteria #5

Practitioners must be able to identify approaches to the education, training and awareness-maintenance of the compliance policy to all staff

Key to this criterion is the ability make training interventions in an informed and planned way. The Compliance function should be proactive in engaging with business leaders, functional managers, and with operational teams. Regular engagement with the business will help paint a clearer picture of where specific training is required, but also what micro-trainings may be necessary to maintain engagement with compliance.

Education in compliance should be viewed as one of the organisation's key regulatory- and compliance-risk controls. Practitioners should be aware that information and data about staff needs for education and training will likely fall within the scope of HR or that departments L&D team. It is therefore important to build strong relationships with HR and develop expertise in defining compliance-competency profiles with them and associated metrics.

The ability to communicate with all staff across a business, supporting a collaborative approach to compliance, is more likely to achieve positive outcomes and build a shared belief in the ability to deliver solutions that are compliant and commercially viable. Tendencies for the Compliance function to be an isolated, remote and aloof second-line operation will limit the impact of compliance.

Performance criteria #6

Practitioners must be able to explain the benefits of compliance policy with reference to examples of good practice within the organisation

This is the opportunity for practitioners to acknowledge the efforts of their colleagues across the organisation to fulfil the aims and objectives of compliance. It also affords an opportunity to investigate and disseminate good practice, by expanding a narrative of compliance and the rewards and/or recognition that this might afford.

It is important, therefore, to keep a record of incidents where good practice is noted. These should be crafted into a narrative about how compliant behaviours safeguard the organisation, ensuring maintenance of integrity, following or establishing market-leading standards that consolidate risk-based regulatory compliance.

Explanations that are going to have traction across the business will need to align with the published values, mission and vision for the organisation. They should be clearly attributable so that the source of evidence can be checked for validity and authenticity by colleagues and other stakeholders. This is important as the veracity of a narrative must be firmly placed within a historical context; otherwise, the explanations become weakened, placed in the domain of fables, and are simply ignored as instructive tales without the real force of actual experience.

Performance criteria #7

Practitioners must be able to communicate the policy across the organisation

It is possible to establish a wide variety of different methods and channels that should be used to communicate a compliance policy. Some of these channels represent an increased risk if protocols are not clear. This can lead to absence or misalignment of communications policies, enforcement of appropriate supervisory procedures and inadequate, incompatible, or incomplete technology and digital solutions, leading to poor compliance outcomes.

Higher risk channels include: conferencing and meeting tools where recording and archiving compliance rules have not been established; instant messaging and collaboration platforms where the volume of data is inadequately managed and control mechanisms are not measured for effectiveness; encrypted channels and mobile phone apps have inadequate or incomplete prohibitions in place (especially if bring-your-own (BYO) technology controls are weak; e.g. for enforcing security updates); and, finally, the extensive use of SMS/text messaging without transparency, disclosure, record-keeping and other controls in place.

Performance criteria #8

Practitioners must be able to ensure that staff have a clear understanding of the regulations that apply to them and their work, and the importance of complying with them

Ensuring that individuals are clear on their requirements, duties and obligations with respect to regulation may be facilitated through the effective use of systems (such as dashboards) and procedures (that could include the use of scripts, schedules and templates), as well as relevant process flows.

Practitioners must work closely with HR colleagues to ensure detailed job descriptions capture regulatory requirements, that induction programmes include relevant compliance duties and obligations (some of which may be contained within an employee handbook and a code of conduct). For financial services professionals, this would also need to align with SM&CR compliance, such as for annual certifications and recertifications.

Where individuals are in higher risk-facing roles, greater efforts must be applied to ensure that compliance is maintained. This may mean closer monitoring of compliance outcomes and that corrective actions are taken where necessary. This may be a distinct focus of Compliance's risk-based approach

Knowledge and understanding criteria

Practitioners need to know and understand a diverse range of legislative and regulatory information, which has grown extensively over recent years. New areas to understand include: sustainability and ESG reporting, digital assets, ultimate beneficial owner (UBO) requirements, new technology requirements.

Perhaps the two most significant aspect of regulatory change commonly held across widely different regulators is the need to ensure that: organisations have in place systems to manage vulnerable consumers; third-party risk management is carried out.

These two areas are expressed in a variety of different regulations. For example:
- the FCA's New Consumer Duty extends the scope of TCF to ensure monitoring of outcomes for vulnerable customers
- Ofgem's amendment to its regulations prohibits back charging by suppliers after 12 months ensuring that vulnerable customers will not have a break in supply caused by a legacy bill
- with the growth of outsourcing, the BoE has introduced a supervisory statement (SS2/21) for outsourcing and third-party risk management
- the Digital Operational Resilience Act (DORA) from the EU specifically addresses cybersecurity threats especially in managing third-party risks.

The diverse range of regulatory knowledge and understanding required for practitioners is extensive

GRC Officers communicate…?

ethical behaviours in the workplace improving the reputation of the sector and market

commitment to compliance with internal and external policies and regulation

excitement about the positive impacts of GRC on stakeholders

welfare of the community you work in and the community you serve

intent to listen and be proactive/active in response

respect for people, who all have a diverse range of life stories

capacity and desire to learn

as an interlocutor with regulators, from the organisation, from the board to staff

a healthy professional self-image

unpopular views when necessary

What does communicating look like in practice?

Skill area: Communicate	Comments (weaknesses/ strengths)
Express unpopular views	A strong understanding of the ramifications of non-compliance may allow someone who lacks self-confidence to deliver bad or unpalatable news when needed.
Ethical behaviours	Simply asking people to follow a Code of Conduct is mechanistic and often fails to gain traction. Promoting ethical behaviours requires hard work including monitoring behaviours and taking assertive action on the evidence.
Commitment to compliance	A strong, consistent and a united front on compliance matters will eventually encourage the most cynical (apart from a minority of rogue players) to comply.
Excitement about positive impacts	Promoting a positive outlook on compliance, showing its benefits to stakeholders, will reduce overall costs and can produce efficiencies by reducing complaints. Timidity about GRC matters will encourage opposition.
Welfare of the community	Generate a shared sense of community through messaging and use of a My Concern framework (or equivalent) and reporting for welfare and vulnerability issues.
Listen to others and encourage a culture of listening	Engage others with interest encouraging them to talk showing interest in what they say, taking positive steps and actions wherever this is possible.
Present a respectful persona	Always be courteous in conversations and encourage polite and iterative dialogue.
Build a learning culture	Demonstrate a desire to learn from others and encourage others to do the same (avoid any signs of hubris); engage with others, and discover the actual feelings about and understanding of, GRC matters.

Communicating compliance

Governance, risk and compliance practitioners must develop a full range of skills from communications (planning, monitoring and so forth) through to the direct tasks of communicating (whether it is in a briefing note or a discussion).

Effective governance, risk and compliance goes beyond simply delivering GRC systems and controls and a risk management framework. Practitioners must become trusted business partners, advising organisations where their exposures are found, the vulnerabilities that exist, and the potential for breaches of regulatory compliance.

A good system in an unethical organisation or with an immature system is likely to lead to poor outcomes, while a more mature organisation, which has poor legacy governance structures or an antiquated compliance management system, may still have better outcomes as the staff within the organisation are keen to ensure good compliance.

The role of the GRC practitioner, then, is pivotal to evolving all aspects of the organisation's development encouraging a tone from the top that builds resilience. A good practitioner is articulate and knowledgeable about legal and regulatory matters but is also able to listen to and address the concerns of individuals struggling to understand the demands of regulation and their role in ensuring compliant activities and behaviours are strong within the organisation.
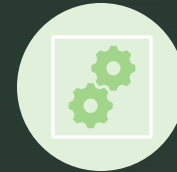
The Concept

Praxis GRC takes an holistic view on competence that considers multiple factors important to their clients:

The degree to which an organisation has reflected on and articulated competence for its stakeholders

The business model and what it aims to achieve and to control

The market, operational and regulatory context

The wider definitions of professional and practitioner best practice

Relevant national occupational standards.

Our consultation, advice, guidance, coaching and mentoring services help evolve clients to their next level, growing into a more mature and resilient organisation better able to deal with volatility and a dynamic environment and business ecology.