BARNOWL

Compliance Software Buyer's Guide

Table of Contents

1. The need for Compliance
2. What do the standards say?
3. The compliance process
4. What will the BarnOwl compliance software do for me?
5. Steps to the successful implementation of compliance software
6. Considerations and key questions when buying compliance software
7. Key feature comparison checklist
8. About BarnOwl

The need for Compliance

Besides the most obvious reason to comply, namely, that it is the law and the risk of penalties, fines, imprisonment, loss of operating license for failing to comply is high, complying with the requirements provides additional benefits to an organisation. Organisations that have effective compliance functions create a competitive advantage for themselves:

- **enhanced client satisfaction and confidence:** There is a direct link between high levels of client satisfaction and confidence for businesses that are perceived to be compliant.
- **management of reputational risk:** An effective compliance function is important in the monitoring and mitigation of reputational risk critical to the sustainability of any business.
- **enhanced investor confidence:** Organisations that have an effective compliance function demonstrate transparency and business integrity, thus enhancing investor and stakeholder confidence.
- **enhanced access to capital and financial markets:** due to improved disclosure and investor confidence
- **higher market value** for the organisation from increased investor confidence
- **better organisational performance:** resulting from 'running a tight ship' with good internal controls
- **enhanced social and environmental standing:** An effective compliance function demonstrates 'good corporate citizenship' necessary for the survival and growth of any organisation.
- **ability to operate in a global business environment:** for an organisation to survive the accelerated dynamics of a global market ('village'), it requires an effective compliance function demonstrating good corporate governance.

In conclusion:

The compliance function plays an invaluable role in any organisation. An organisation should establish an independent compliance function as part of its risk management framework in order to ensure that the organisation continuously and effectively manages the various compliance risks that apply to the organisation and the industry in which it operates. The function is relied upon to assist the top management and management of the organisation in complying with the ever-increasing regulatory requirements. The role of the compliance function is to find a balance between meeting regulatory requirements that demand compliance without impacting on the business imperatives of the organisation negatively.

What do the standards say?

King IV

The King IV code on corporate governance (copyright Institute of Directors Southern Africa) applies to all entities, regardless of their nature, size or form of incorporation. The Code is implemented on an "apply and explain" basis. The following principles relating to compliance governance are embodied in the Code:

- Strategy, Performance and Reporting: Principle 4: The governing body should appreciate that the organisation's core purpose, its risk and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process.

- Compliance Governance: Principle 13: The governing body should govern compliance with applicable laws and adopted, non-binding rules, codes and standards in a way that supports the organisation being ethical and a good corporate citizen.

Recommended Practices

18. The governing body should assume responsibility for the governance of compliance with applicable laws and adopted, non-binding rules, codes and standards by setting the direction for how compliance should be approached and addressed in the organisation.

What do the standards say?

19. The governing body should approve policy that articulates and gives effect to its direction on compliance, and that identifies which non-binding rules, codes and standards the organisation has adopted.

20. The governing body should delegate to management responsibility for implementation and execution of effective compliance management.

21. The governing body should exercise ongoing oversight of compliance and, in particular, oversee that I results in the following:
    a. Compliance being understood not only for the obligations it creates, but also for the rights and protections it affords
    b. Compliance management taking a holistic view of how applicable laws and non-binding rules, codes and standards relate to one another
    c. Continual monitoring of the regulatory environment and appropriate responses to changes and developments

22. The governing body should consider the need to receive periodic independent assurance on the effectiveness of compliance management.

23. The following should be disclosed in relation to compliance:
    a. An overview of the arrangements for governing and managing compliance
    b. Key areas of focus during the reporting period
    c. Actions taken to monitor the effectiveness of compliance management and how the outcomes were addressed
    d. Planned areas of future focus
24. Material or repeated regulatory penalties, sanctions or fines for contraventions of, or non-compliance with, statutory obligations, whether imposed on the organisation or on members of the governing body or officers should be disclosed.
25. Details of monitoring and compliance inspections by environmental regulators, findings of non-compliance with environmental laws, or criminal sanctions and prosecutions for such non-compliance should be disclosed.

Generally Accepted Compliance Practice Framework (GACP) developed by The Compliance Institute Southern Africa:

The Compliance Institute Southern Africa has developed a Generally Accepted Compliance Practice Framework (GACP). The objective of the GACP is to provide compliance practitioners and other interested stakeholders, with a set of compliance principles, standards and explanations as well as a Code of Ethical and Professional Conduct. The objective of this framework is to provide a benchmark of compliance best practice thereby enhancing the applications and professionalism of compliance practitioners in South Africa. The following principles and standards are set out in the Generally Accepted Compliance Practice Framework (GACP):

- **Principles and standards 1: governance:** As ultimate responsibility for understanding and overseeing the management of compliance with the applicable regulatory requirements resides with the top management of an organisation, this responsibility should be recognised in the governance structures of the organisation.

- **Principles and standards 2:** compliance policy: A written compliance policy should exist, which sets out the organisation's commitment and approach to compliance, as well as what is expected of all employees. The compliance policy should include a compliance policy statement.

- **Principles and standards 3:** responsibility of management: Management is responsible for ensuring that the compliance policy is implemented, supported and adhered to.

- **Principles and standards 4:** establishment of a compliance function: The organisation should establish a permanent and effective compliance function in terms of its compliance policy.

- **Principles and standards 5:** status: The status of the compliance function should be spelt out in the compliance policy or charter that clearly sets out its authority, independence, role and responsibilities.

- **Principles and standards 6:** independence: The compliance function should be sufficiently independent of business activities to be able to discharge its responsibilities objectively.

Generally Accepted Compliance Practice Framework (GACP) developed by The Compliance Institute Southern Africa:

- **Principles and standards 7:** roles and responsibilities: The primary role of the compliance function is to assist top management, management and appropriate staff members in discharging their responsibilities to comply with applicable regulatory requirements through the provision of compliance risk management services.

- **Principles and standards 8:** head of compliance: The organisation should assign responsibility for the day-to day management of the compliance function to a senior person.

- **Principles and standards 9:** fit and proper: Compliance staff should have the qualifications, experience and personal qualities to carry out their duties effectively.

- **Principles and standards 10:** resources: The compliance function should have adequate resources including human, financial and operational capacity.

- **Principles and standards 11:** appointment and termination: The appointment of staff members responsible for compliance management should follow a formal appointment process, and termination should be subject to appropriate governance/oversight requirements.

- **Principles and standards 12:** compliance culture: An appropriate compliance culture, including desired ethical behaviour, should be promoted throughout the organisation.

- **Principles and standards 13:** outsourcing: Compliance services may be outsourced to an independent compliance officer (ICO) subject to appropriate oversight and provided that top management remains ultimately responsible for compliance within the organisation.

- **Principles and standards 14:** independent review: The compliance function should be subject to regular independent review

Generally Accepted Compliance Practice Framework (GACP) developed by The Compliance Institute Southern Africa:

- **Principles and standards 15:** materiality: The organisation should determine levels of materiality (quantitative and qualitative) through the assessment of compliance risks and their impact on business objectives.

- **Principles and standards 16:** compliance process: Organisations should have a compliance process in place that includes effective monitoring practices.

The compliance process:

As per the GACP framework, "The compliance process should encompass compliance risk identification, compliance risk assessment, compliance risk management and compliance monitoring. This plays an essential role in assisting management to discharge its responsibility to comply with applicable regulatory requirements."

Phase I - compliance risk identification

1.1 Identify all the applicable requirements that fall within the scope of the compliance risk for the entity as a whole. (This should be done first for the entity as a whole and thereafter for the individual divisions/subsidiaries).

Phase II - compliance risk assessment

2.1 Categorise the identified requirements in terms of core/primary, secondary or topical/ pertinent.
2.2 Prioritise the identified requirements by rating each in terms of Probability and Seriousness. (The provisions of each requirement should also be analysed and prioritised, if applicable, on the same basis)
2.3 Plot the requirements according to the ratings on a scatter diagram (if needed).
2.4 Classify requirements into high, medium and low risks

Phase III - compliance risk management (control optimisation)

3.1 Based on the requirements in the high risk area as priority, develop a compliance risk management plan for each requirement by identifying, inter alia, the following:
- the provision(s) for each requirement that has to be complied with;
- the control measure that will monitor compliance;
- the responsible person for implementing the control measure;
- the target date for implementing the control measure (if applicable)

3.2 Include compliance risk management plan in the compliance manual.

The compliance process:

Phase IV - compliance risk monitoring

4.1 Develop an effective review process to evaluate the implementation of the compliance risk management plans throughout the entity. This would include the development of a compliance risk monitoring plan.

4.2 Monitor in terms of the review process and report findings to the relevant role-players.

What will the BarnOwl compliance software do for me?

The BarnOwl compliance module facilitates the compliance process by:

- greatly reducing the administrative burden of compliance,
- enabling you to manage and keep up to date all acts, regulations and provisions as they pertain to your organisation
- embedding a culture of compliance in your organisation with the automation of compliance checklists, control self-assessments, 'living' action plans,
- providing an early warning system where there is non-compliance,
- ongoing monitoring of your compliance environment,
- assisting with regulatory and management reporting,
- limiting director exposure through a formalised approach to risk and compliance management.

The BarnOwl compliance module enables an organisation to manage its regulatory universe by facilitating and automating to a large extent the identification, rating and monitoring of compliance to the acts, regulations and provisions at every level of the organisation, where applicable. Compliance legislation can be imported directly into BarnOwl from third party content providers such as Lexis Nexis or EoH Legal and / or can be populated with your own compliance content including internal policies, procedures etc. Updates to the regulations and provisions can be uploaded into BarnOwl automatically.

What will the BarnOwl compliance software do for me?

BarnOwl supports and facilitates the compliance process as follows:

- Phase I – Compliance Risk Identification: BarnOwl enables you to:
  - o import (automatically from 3rd party content providers) a library of acts, regulations and provisions (requirements) which are applicable to your organisation as a whole and for the individual divisions/subsidiaries.

- Phase II – Compliance Risk Assessment: BarnOwl enables you to:
  - o categorise the identified acts in terms of core/primary, secondary or topical/pertinent for the organisation as whole and for the individual divisions/subsidiaries,
  - o prioritise the identified acts by rating each in terms of Probability and Seriousness for the organisation as whole and at the various levels of the organisation where applicable,
  - o plot the requirements according to the ratings on a scatter diagram (rainbow chart),
  - o create and rate (prioritise) the provisions / compliance risks at the various levels of the organisation based on Impact and Likelihood in line with best practice enterprise risk management.

- Phase III – Compliance Risk Management (Control optimisation): BarnOwl enables you to:
  - o generate compliance risk management plans based on the requirements in high risk areas by identifying, inter alia, the following:
    - the provision(s) for each requirement which has to be complied with,
    - the control measure that will monitor compliance,
    - the responsible person for implementing the control measure (automated risk and control self-assessments (CSAs) sent to the relevant control owner/s to rate control adequacy and effectiveness) and attach evidence,
    - the target date for implementing the control measure (action plans with automated email notifications, reminders and escalation sent to the relevant action plan owner/s),
    - automated CSAs and compliance checklists sent to the relevant owner/s as per the compliance schedule.

What will the BarnOwl compliance software do for me?

- Phase IV – Compliance Risk Monitoring: BarnOwl:
  - monitors action plan activity by owner and due date,
  - enables a review process of risk & control self-assessments and compliance checklists. In addition, the BarnOwl Internal Audit (IA) module which is fully integrated with the risk and compliance modules enables independent testing of compliance controls and the raising of non-compliance findings,
  - provides extensive compliance reporting: compliance risk and control ratings, non-compliance findings, issues, overdue action plans,
  - also enables you to maintain and track tip-offs, issues, loss events, complaints, gifts, conflicts of interest related to the compliance function.

Steps to the successful implementation of compliance software

Preparation before implementing software:

1. Benchmark your compliance function against the principles and standards listed above as set-out by Generally Accepted Compliance Practice Framework (GACP) developed by The Compliance Institute Southern Africa. Although organisations may not have a fully developed and mature compliance function, it is important that they are constantly working towards that goal through the implementation and monitoring of a coherent compliance strategy rather than being in reactive mode where compliance is not regarded as a priority.

2. Identify the acts, regulations and provisions (within the act) applicable to your organisation as a whole and thereafter for the individual divisions/subsidiaries.

3. Collate your own compliance content or consider purchasing 3rd party compliance content in BarnOwl importable format (Excel in prescribed format).

4. Confirm buy-in from the top and educate relevant stakeholders as to their role in the compliance process and how the system will impact them (i.e. automated action plans, automated compliance risk & control self-assessments, online checklists etc.)

Using the software:

1. Use BarnOwl to facilitate the compliance process outlined above.

2. Embed and expand the usage of the system over time. Apply and monitor the relevant acts and provisions for each of the business divisions / subsidiaries

3. Demonstrate effective mitigation / reduction of compliance risks and controls and the avoidance of associated consequences

4. Follow up on remedial action plans

5. Maintain and monitor issues, findings etc.

6. Proactive reporting and monitoring

Considerations and key questions when buying compliance software

- Does the software support best practice standards (such as GACP (Generally Accepted Compliance Practice Framework), COSO, ISO31000)
- Does the system easily support and facilitate the compliance process as set-out in the standards
- Is the system fully integrated with enterprise risk management and audit and does the system support risk-based compliance
- Does the system provide up-to-date legislative compliance content which is easily imported and kept up to date in the system
- Does the solution provide a simple, cost effective, user friendly and non-intrusive interface for the average business user? E.g. action plans, checklists, risk& control self-assessments etc.
- Is the system flexible, configurable and parameter driven in order to support your risk and compliance methodology
- Ensure that the software offers flexible reporting capability without any programmer intervention
- Apart from the standard features, what differentiators / value add does the software offer
- What is the setup process and estimated timelines; it should be easy to get up and going with the software
- Is the system fully documented, user manuals, online help, FAQs (Frequently Asked Questions)
- Is there local support and how responsive are the software owners and developers to your changing requirements
- Are there any hidden fees or costs (e.g. hosting, support, additional implementation, other required 3rd party software licenses, online action plan users etc?)

Considerations and key questions when buying compliance software

- Ensure that there are regular upgrades to the software ensuring that it is aligned with best practice risk and compliance standards as well as kept up to date with the latest technology platforms and that the upgrade process is simple and never corrupts existing custom fields / custom settings.

- Request client references / testimonials

Key feature comparison checklist

Use this comparison checklist to compare important feature sets from competing software solutions:

Important features	BarnOwl	Software B	Software C
Is the system a fully integrated GRC software solution offering integrated modules such as compliance, enterprise risk management, incident management and audit	✓		
Does the system offer full system functionality supporting best practice standards (such as GACP, COSO, ISO31000) including functionality to maintain acts, regulations, provisions, automate compliance risk management plans (CRMPs), identify controls (including multi-rating of controls per assurance provider), contributing factors, KRIs, incident / issue management, action plans, voting, risk & control self-assessments, compliance checklists, questionnaires.	✓		
Does the system easily support and facilitate the compliance process as set-out in the standards	✓		
Simple and flexible take-on / import of compliance content (acts, regulations, provisions, checklists) and subsequent updates	✓		

Key feature comparison checklist

Important features	BarnOwl	Software B	Software C
Automatic generation of compliance risk management plans	✓		
Automatic generation of online compliance checklists	✓		
Risk-based compliance	✓		
Automated follow up on remedial action plans (email notifications, reminders, escalation)	✓		
Highly flexible and customisable report generation without any programmer intervention	✓		
Combined assurance reporting	✓		
Graphical slice and dice reporting: e.g. compliance heat-map (scatter diagram), risk heat map, heat map movement, trends, risk ranking, causal analysis, etc.	✓		
User-defined fields available anywhere in the system and ability to report on user-defined fields	✓		
Automated risk & control self-assessments without any licensing or cost implications	✓		

Key feature comparison checklist

Important features	BarnOwl	Software B	Software C
Online questionnaires and checklists without any licensing or cost implications	✓		
Online action plans with email notifications to all compliance control owners without any licensing or cost implications	✓		
Addition module/s for incident management, issue tracking, complaints, tip offs (whistle blowing), loss events, conflict of interest register, gifts register etc.	✓		
Ease of use including a 'Lite' offering allowing easy adoption and buy-in for the system by the business users.	✓		
User / Group security restricting unit and risk owner access	✓		
Ability and willingness of the vendor to respond to software enhancement requests	✓		
Online help, FAQs, up-to-date system documentation	✓		
End user support process, support portal	✓		

Key feature comparison checklist

Important features	BarnOwl	Software B	Software C
Regular and seamless software upgrades	✓		
Client references and track record of the vendor	✓		

About BarnOwl

BarnOwl is a fully integrated governance, enterprise risk management, compliance and audit software solution used by over 200 organisations in Africa, Europe and the UK. BarnOwl supports best practice risk management, compliance and audit frameworks (e.g. COSO, ISO31000, Compliance Institute's handbook, International Professional Practice Framework), whilst offering a highly flexible and configurable parameter-driven system allowing you to configure BarnOwl to meet your specific requirements.

www.barnowl.co.za

Acknowledgements to The Compliance Institute of Southern Africa and to the King Committee on Corporate Governance