ISO 19600 COMPLIANCE
Certified System

COMPASS
-ASSURANCE SERVICES-

ISO19600:2014: COMPLIANCE MANAGEMENT SELF ASSESSMENT CHECKLIST

COMPASS ASSURANCE SERVICES PTY LTD

NOTE: THIS IS A SIMPLIFIED SUMMARY OF THE REQUIREMENTS OF ISO 19600:2014 COMPLIANCE MANAGEMENT SYSTEM – REQUIREMENTS FOR THE SPECIFIC PURPOSE OF HELPING ORGANISATIONS UNDERTAKE A PRELIMINARY CHECK OF THEIR READINESS FOR AN ISO 19600:2014 COMPLIANCE AUDIT OR ASSESSMENT.

ISO 19600 COMPLIANCE
Certified System

COMPASS
-ASSURANCE SERVICES-

ISO19600:2014: COMPLIANCE MANAGEMENT

ISO19600:2014 helps establish, develop, evaluate, and maintain a compliance management system. The extent of the application of these guidelines depends on the size, structure, nature and complexity of the organization. ISO 19600:2014 is based on the principles of good governance, proportionality, transparency and sustainability

KEY DOCUMENTS

- [ ] Scope of the Compliance Management Systems (CMS)
- [ ] Compliance obligations and plans to achieve
- [ ] Compliance Policy
- [ ] Compliance risks and plans to address
- [ ] Employee competency records
- [ ] Audit programme and audit results
- [ ] Results of management review
- [ ] Non-conformances and actions taken
- [ ] Results of monitoring activities

4. CONTEXT OF THE ORGANIZATION

- ☐ Do we understand the external and internal issues related to compliance?
- ☐ Have we determined interested parties and their requirements?
- ☐ Have we determined the scope of the system and documented it?
- ☐ Does our CMS reflect the organisation's values, objectives, strategy and compliance risks?
- ☐ Have we identified our compliance obligations and their implications and documented this?
- ☐ Do we have a process to identify changes to law and other obligations and do we evaluate these changes and implement changes as appropriate?
- ☐ Have we identified, analysed and evaluated compliance risks? Do we re-assess when changes or issues occur?
- ☐ Is the compliance function independent and have the authority to act?

5. LEADERSHIP

- ☐ Do the board and top management demonstrate commitment to the CMS by;
  - ☐ setting core values,
  - ☐ ensuring compliance policy and objectives established,
  - ☐ ensure resources are available,
  - ☐ ensure CMS is integrated and consistent with other processes,
  - ☐ communicating the importance of the CMS,
  - ☐ establishing reporting mechanisms and
  - ☐ effectively ensuring the CMS achieves its outcomes?
- ☐ Have we established a Compliance Policy that sets a framework for objectives, a commitment to meet requirements and for continual improvement?
- ☐ Does the policy articulate the scope, extent of integration, autonomy of the compliance function, principles for managing internal and external relationships, along with standards of conduct and accountability?
- ☐ Is the policy documented in plain language and translated as necessary, communicated within the organization, available to interested parties as appropriate and updated?

- [ ] Are responsibilities for compliance assigned and communicated?
- [ ] Has the board and top management:
  - [ ] established policy,
  - [ ] ensured commitment to compliance is maintained,
  - [ ] non-compliance is dealt with,
  - [ ] ensured compliance responsibilities are in top management position statements,
  - [ ] appointed a compliance function with appropriate authority and resources?
- [ ] Does the compliance function with management have responsibility for;
  - [ ] identifying obligations and acting on them,
  - [ ] integrating compliance into processes,
  - [ ] providing training to support employees,
  - [ ] establishing compliance reporting processes,
  - [ ] establishing processes for complaints/hot-lines/whistle-blower as appropriate,
  - [ ] establishing performance indicators,
  - [ ] identifying and managing risks,
  - [ ] reviewing the CMS, providing employees with information and advice,
  - [ ] ensure access to professional advice as required?
- [ ] Do managers have responsibilities for compliance within their area of responsibility including job descriptions and performance appraisals?
- [ ] Are all employees aware of their responsibilities including adhering to obligations, participate in training, use compliance resources, report compliance concerns?

6. PLANNING

- [ ] Are plans in place to address compliance risks?
- [ ] Are the risks and plans to address them documented?
- [ ] Do we have documented compliance objectives at relevant levels and functions and plans to achieve them?

7. SUPPORT

- [ ] Have we determined what resources are required and deployed them to ensure the system is effective, objectives are achieved and compliance achieved?

- [ ] Have we determined the necessary competence of employee(s) related to Compliance and taken action as necessary? Have we retained documented information as evidence?
- [ ] Do we have a training program to ensure that all employees are competent to fulfill their job role consistent with the organization's commitment to compliance?
- [ ] Have we ensured all persons doing work are aware of the compliance policy, their role and contribution to the CMS and implications of not conforming?
- [ ] Is behaviour that creates and supports compliance encouraged and behaviour that compromises compliance not tolerated?
- [ ] Has the board, top management and management committed towards a common, published standard of compliance behaviour that is required throughout every area of the organization?
- [ ] Have we adopted appropriate methods of communication to ensure that the compliance message is heard and understood by all employees on an on-going basis?
- [ ] Have we put in place a practical approach to external communication, targeting all interested parties, as appropriate?
- [ ] Are internal and external documents relating to the CMS approved for use and protected adequately?

8. OPERATION

- [ ] Do we control planned changes and review the consequences of unintended changes relevant to the CMS?
- [ ] Have we established controls and procedures to manage obligations and associated risks to achieve desired behavior?
- [ ] Are these controls maintained, periodically evaluated, and tested to ensure their continuing effectiveness?
- [ ] Have we established, documented, implemented and maintained procedures to support the compliance policy and translate the compliance obligations into practice?
- [ ] Have we ensured outsourced processes are controlled and monitored?
- [ ] Do we have specific arrangements for identifying, reporting and escalating noncompliance and risks of noncompliance?

9. PERFORMANCE EVALUATION

- [ ] Do we evaluate the CMS performance and effectiveness?
- [ ] Have we established a plan for;
  - [ ] continual monitoring,
  - [ ] setting out monitoring processes,
  - [ ] schedules,
  - [ ] resources and
  - [ ] the information to be collected?
- [ ] Do we consider effectiveness of training, controls, responsibilities, currency of obligations?
- [ ] Do we monitor;
  - [ ] noncompliance and "near misses",
  - [ ] instances where obligations or objectives are not met,
  - [ ] status of compliance culture and,
  - [ ] leading and lag indicators?
- [ ] Do we have procedures for seeking and receiving feedback on compliance performance from stakeholders such as employees, customers, suppliers, regulators and from control logs and activity records?
- [ ] Do we have information management systems for capturing issues and complaints that allow classification and analysis of those that relate to compliance?
- [ ] Have we a set of measurable indicators that assist in measuring achievement of our objectives and quantifying compliance performance?
- [ ] Is the board and top management effectively informed in a timely manner on the performance of the CMS and all relevant noncompliances?
- [ ] Are employees encouraged to respond to and report noncompliances without fear of retaliation?
- [ ] Do we maintain accurate, up-to-date records of our compliance activities and for complaints, disputes and alleged noncompliance and the steps taken to resolve them?
- [ ] Do we conduct audits of our CMS at planned intervals and retain documented information as evidence?

- [ ] Do our information systems capture issues and complaints with the ability to classify and analyse those that relate to compliance?
- [ ] Do we have compliance reporting that has appropriate criteria and obligations?
- [ ] Does top management review our CMS at planned intervals to ensure its continuing suitability adequacy and effectiveness including;
  - [ ] consideration of previous actions,
  - [ ] policy,
  - [ ] objectives,
  - [ ] resourcing,
  - [ ] changes,
  - [ ] performance measures,
  - [ ] non-conformance,
  - [ ] audit results, and
  - [ ] stakeholder communication?
- [ ] Does the output of management review include;
  - [ ] recommendations on policy,
  - [ ] objectives,
  - [ ] structures,
  - [ ] personnel,
  - [ ] changes to processes,
  - [ ] areas to be monitored,
  - [ ] corrective action to non-conformance,
  - [ ] gaps in systems and
  - [ ] recognition of exemplary behavior?
- [ ] Do we maintain documented information of this and provide the board a copy?

10. IMPROVEMENT

- [ ] When a nonconformity and/or noncompliance occurs do we;
  - [ ] take action to control and correct,
  - [ ] manage the consequences,
  - [ ] evaluate need to eliminate cause,
  - [ ] implement actions,
  - [ ] review effectiveness of corrective action and
  - [ ] make changes to system as necessary?

- [ ] Do we retain documented information on non-conformances and actions taken and results of the action?
- [ ] Do we have a clear and timely escalation process that ensures that all noncompliances are raised, reported and escalated to relevant management, and that the compliance function is informed and able to support the escalation?
- [ ] Where we are required by law to report noncompliance, do we ensure regulatory authorities are informed in accordance with the applicable regulations or as otherwise agreed?
- [ ] Do we continually improve the suitability, adequacy and effectiveness of the CMS?

- END OF DOCUMENT -