CORPORATE COMPLIANCE AUDIT PROGRAMS AND CHECKLISTS

By John Kyriazoglou* (author’s credentials at the end of this document)

The following audit program and checklists are designed to be used by managers, auditors and compliance staff in the process of establishing, controlling, reviewing, assessing and auditing the corporate compliance area and its particular components (compliance policies and procedures, corporate policies and procedures, ethics aspects, etc.).

The following audit programs and checklists, as detailed in the following paragraphs, should be reviewed and customized before they are used in any corporate environment:

1. Corporate governance and internal controls systems audit program,
2. Assessment of the compliance controls framework,
3. Corporate policies and procedures checklist,
4. Records management system checklist,
5. Financial management system checklist,
6. Corporate fraud management system checklist,
7. Internal audit checklist, and
8. Ethics management checklist

1 Corporate governance and internal controls system audit program

1. Assess Board and senior executive management responsibility for the oversight and monitoring of corporate governance and internal controls.

Consider: Board and senior management should ensure that policies, procedures and systems are current and well documented. Management should establish an effective system of internal controls. Corporate, compliance, risk management and internal controls should cover the IT environment as well as the other business functions. Board and senior management should adopt and enforce appropriate policies and procedures to manage compliance, all risks (enterprise, IT, investments, etc.), and should re-evaluate and improve these controls every year or two.
2. Assess senior executive management practices.

Consider: Reporting effectiveness to the Board of Directors. Periodic review and updating of policies, standards, procedures and practices. Instituting controls to ensure that management information and detailed data are reliable and the reporting cycle is adequate, and that operating procedures are efficient and effective. Regular review of compliance issues, risks, segregation of duties, personnel controls, information security, software development and acquisition, outsourcing, insurance issues, internal and external audit results, service level agreements and performance measurements including issues and corrective action plans, ensuring that procedures are in effect to assure continuity of business, etc.

3. Does the internal controls framework identify all the required control components?

Consider: Control environment, risk assessment control activities information and communication monitoring.

4. Do the key functions of internal controls relate to all critical elements of governance?


5. Do internal controls contain all types of controls?

Consider: Preventive controls (e.g. division of duties, authorization levels), detective controls (e.g. stock verification, bank reconciliation), directive controls (e.g. policies, procedures, training).

6. Are there adequate and effective financial controls in place at the detailed level, as required?

7. Are there adequate and effective customer service controls in place at the detailed level, as required?

8. Are there adequate and effective production/manufacturing controls in place at the detailed level, as required?

9. Are there adequate and effective information and communications controls in place at the detailed level, as required?
10. Are there adequate and effective asset management controls in place at the detailed level, as required?

11. Are there adequate and effective sales management controls in place at the detailed level, as required?

12. Are there adequate and effective management reporting controls in place at the detailed level, as required?

13. Are there adequate and effective internal audit controls in place at the detailed level, as required?

14. Are there adequate and effective human resource management controls in place at the detailed level, as required?

15. Are there adequate and effective research and innovation controls in place at the detailed level, as required?

16. Is there a formal and well-established performance management system for all functions of the organization?

Consider: The performance management system should promote and accelerate the rate of successful changes, increase the predictive and early warning capabilities to management, provide a holistic perspective to the management of the organization, link to the reward and other incentive systems of the organization, link and align on an integrated mode to the objectives and measures of the other corporate levels of the organization, such as: division, department, business unit, process, function, project, teams, etc.

17. Are critical performance data shared across all levels of the organization?

18. Are strategic performance data reviewed at the appropriate levels of the organization, and actions taken as necessary?

19. Are the approved personnel empowered to have access to whatever critical performance data is required to make balanced decisions?

20. Is the accountability and follow-through process based on critical performance data?

21. Is the psychological resistance of staff (management, line staff, etc.) managed and resolved accordingly?

22. Is there an active audit committee in place?
23. Is there an internal audit function in place?

24. Is there a compliance function in place with all its constituent components (compliance officer, compliance committee, policies, procedures, action plan, etc.)?

25. Are corrective and improvement measures taken when performance issues and compliance breaches occur?

2. Assessment of the compliance controls framework

Assess the organizational structure to ensure that it is neither so simple that it cannot adequately monitor the entity’s activities nor so complex that it inhibits the flow of necessary information.

1. Does the compliance monitoring system of the organization cover all business functions?

2. What is the management’s attitude towards compliance with laws and regulations?

3. Does the management of the organization specify the level of competence needed for particular jobs, and translate the desired levels of competence into requisite knowledge, cultural characteristics and skills?

4. Does the Board or governing council provide an effective oversight function to ensure that the management of the organization does not override system controls?

5. Is the philosophy and operating style of management compliance-related?

6. Does the assignment of responsibility, delegation of authority and establishment of related policies and procedures provide a basis for effective accountability and control?

7. Are human resources policies the basis for recruiting and retaining competent people to enable the plans of the organization to be carried out and its goals and objectives to be achieved?

8. Does the Board, the senior executives and the management of the organization have a clear understanding of all strategic components, and convey the message that integrity and ethical values of the organization cannot and should not be compromised by anyone?

Consider: Clear understanding of the values, mission and vision, and performance targets of the organization. Full understanding of the general goals and specific objectives of the organization and how they fit in the
framework of corporate strategy. Provision of adequate information for risk identification and resolution. Clear understanding of the role played by policies and procedures in achieving effective controls and compliance.

3. Corporate policies and procedures checklist

1. Have compliance rules, guidelines, policies and procedures been formally established and communicated to all levels and functions of the organization?

2. Is there an approved performance policy, system and evaluation process in place?

3. Is there an approved human resources management policy, set of procedures, a system and an evaluation process in place?

4. Is there an approved financial and cost management policy, and a set of related procedures in place?

5. Is there an approved asset management, disposition and protection system in place?

6. Is there an approved IT policy and a set of related procedures covering all areas, such as strategy, security, contingency planning and disaster recovery, information systems development and operation, database and data privacy protection, web services, etc.?

7. Is there an approved research and innovation system in place?

8. Is there a Management Reporting System (MRS) in place?

9. Is there a quality management system in place?

10. Is there a risk management system in operation?

11. Is there an ethics code and policy in place?

12. Is there a compliance policy in place?

13. Is there a corporate social responsibility policy in place?

14. Is there an anti-fraud policy in place?

4. Records management system Checklist

1. Have operational guidelines and manuals been formally established, communicated to all levels and functions of the organization, and used in every-day work by all personnel?
2. Does the record-keeping system (for both manual and computerized files, media and data) of the organization produce complete and accurate results?

3. Is there an adequate documentation and effective audit trail for all transactions and activities?

4. Is there an approved segregation of duties policy, and a set of related procedures in operation?

5. Is there an approved employee rotation policy for critical jobs/tasks in operation?

6. Have levels of authorization been defined for all levels of management and all transactions and activities?

7. Are adequate asset protection and disposition controls in operation?

8. Are effective financial and cost management controls in operation?

9. Is there an active security committee, policy and procedures (for all elements: data, plants, installations, offices, infrastructure, systems, records, files, etc.) in operation at all levels?

10. Is there an active performance and compliance management, measurement and exception reporting system in place?

5. Financial management system checklist

1. Does the organization have a system for recording and tracking commitments, obligations and expenditures, and reconciling financial data?

2. Does the organization have controls that prevent incurring obligations in excess of funds available within a budget cost category?

3. Does the organization have a mechanism to ensure that periodic audits of the financial management area are undertaken?

4. Does the organization adjust financial plans in the light of the actual operating budget?

5. Does the organization monitor the reliability and confidentiality of financial data used in mission critical budgetary decisions?

6. Does the organization guard against breaches in confidentiality and loss of budget data integrity?
7. Does the organization use an operating budget to control project funds?
8. Does the organization link strategic goals, objectives and operational performance targets to budget performance activities?

**6. Corporate fraud management system checklist**

1. Does the organization have, within the corporate ethics policy, a statement with respect to fraud?

   Consider: fraud definition, fraud hot-line, applicability to all employees, management, Board members, external contractors, media communications procedure for a disciplinary interview, employee services termination procedure, obligations of employees during notice periods and upon termination of employment, complaints procedure, conflict resolution, insurance claims, police contacting issues, investigation of fraud and corruption, theft and threats policy, obligations of external contractors, investigating procedure by the use of external approved investigators or expert internal audit personnel, and the protection procedure for the information sources.

2. Who is responsible for the issue of this statement?

3. Has this policy statement been approved and ratified by the Board or other top management committee?

4. Is this statement widely publicized in the organization?

5. Is this statement reviewed and improved annually?

6. Is the policy statement linked to internal controls?

7. Who (manager, function, etc.) is responsible for ownership and administration of the fraud policy?

8. How are fraud risks monitored, e.g. through risk registers?

9. Is there a budget for investigative costs on potential fraud issues?

10. Does the organization specify roles and responsibilities within the fraud policy (e.g. for the audit committee, the Board, the HR function, a Fraud Liaison Officer, etc.)?

11. What is the procedure for reporting suspicions of fraud?

12. What guidance is provided on dealing with incoming mail (such as anonymous letters, e-mails, etc.)?
13. Who are the first points of contact for reporting suspected dishonesty?

14. Does the organization have a whistle-blowing policy, which sets out the principles for protection of employees when reporting suspicions?

15. Does the organization keep a register of fraud?

16. Who is responsible for maintenance of this register (e.g. a Fraud Officer)?

17. What are the access rights to the fraud register?

18. Is the fraud register held securely?

19. Who is responsible for the investigation (e.g. internal audit)?

20. Who oversees the investigation?

21. Do written reports have to be submitted and to whom?

22. Are employees suspended from work pending an investigation?

23. Are all reasonable means of recovering any identified loss pursued?

7. **Internal audit checklist**

1. **Is there an internal audit department?**

   Consider: terms of reference, organization chart, independence, expertise in IT.

2. **Is there an internal IT audit function?**

   Consider: IT audit plan, adequacy of resources, suitability of resources, including qualifications, experience, technical competence and training.

3. **Is there an internal audit policy document?**

   Consider: standards regarding review objectives, work plan, documentation, conclusions, report format, manager review.

4. **Are all compliance issues subject to independent review by an internal audit function?**

   Consider: involvement in reviewing system developments, existing systems, computer operations, security and control issues use of audit software, etc.
8. Ethics management checklist

1. Does a code of ethics exist for all personnel, including IT?
2. Has an anti-fraud policy and associated procedures been put into operation for the organization?
3. Are confidentiality statements signed by all IT personnel and all critical users?
4. Do explicit corporate rules cover issues, such as:
   Personal use of computer services,
   proprietary rights to computer programs,
   proprietary rights to data,
   confidentiality of passwords,
   physical access to restricted areas,
   management of visitors,
   use of terminals,
   personal use of media and supplies,
   disclosure of privileged information,
   maintenance of professional relationships,
   reporting mechanism for conflict situations,
   penalties and rewards for violators,
   clear assignments of accountability,
   controls over data and files,
   Data Protection Act,
   data classification system?
5. Is there a centralized ethics control function?
6. Are proper international ethics standards used in the design and implementation of the code of ethics of the organization?

7. Is there an ethics program and appointed staff in implementation or operation?

8. Have all staff undertaken, or are there schedules for, ethics training?

*Author’s Credentials*

John Kyriazoglou, CICA, M.S.,B.A(Hon), is an International IT and Management Consultant, author of the book ‘IT STRATEGIC & OPERATIONAL CONTROLS’ (published in 2010 by www.itgovernance.co.uk), and co-author of the book CORPORATE CONTROLS’ (to be published in 2/2012 by www.theiic.org), with Dr. F. Nasuti and Dr. C. Kyriazoglou.

E-Mail: jkyriazoglou@hotmail.com
Profiles
http://www.linkedin.com/pub/john-kyriazoglou/0/9b/919
http://www.authorsden.com/jkyriazoglou
http://www.icttf.org/profile/johnkyriazoglou
http://www.blogger.com/profile/15482029934015594259
Blogs
Articles, Opinions, etc.: http://corporatecontrols.blogspot.com/
Publications: http://johnkyriazoglou-works.blogspot.com/