Handout for Compliance Professionals
Roles & Responsibilities

In corporate world compliance professionals are considered as protection shield and safeguard of business entities particularly shareholders, management, employees and third parties associated with business. Compliance professional can mitigate information technology challenges performing following functions.

1. Risk Identification, Assessment and Evaluation

Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy.

- Collect information and review documentation to ensure that risk scenarios are identified and evaluated.
- Identify legal, regulatory and contractual requirements and organizational policies and standards related to information systems to determine their potential impact on the business objectives.
- Identify potential threats and vulnerabilities for business processes, associated data and supporting capabilities to assist in the evaluation of enterprise risk.
- Create and maintain a risk register to ensure that all identified risk factors are accounted for.
- Assemble risk scenarios to estimate the likelihood and impact of significant events to the organization.
- Analyze risk scenarios to determine their impact on business objectives.
- Develop a risk awareness program and conduct training to ensure that stakeholders understand risk and contribute to the risk management process and to promote a risk-aware culture.
- Correlate identified risk scenarios to relevant business processes to assist in identifying risk ownership.
- Validate risk appetite and tolerance with senior leadership and key stakeholders to ensure alignment

2. Risk Response

Develop and implement risk responses to ensure that risk factors and events are addressed in a cost-effective manner and in line with business objectives.

- Identify and evaluate risk response options and provide management with information to enable risk response decisions.
- Review risk responses with the relevant stakeholders for validation of efficiency, effectiveness and economy.
- Apply risk criteria to assist in the development of the risk profile for management approval.
- Assist in the development of risk response action plans to address risk factors identified in the organizational risk profile.

3. Risk Monitoring

Monitor risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy.

- Collect and validate data that measure key risk indicators (KRIs) to monitor and communicate their status to relevant stakeholders.
- Monitor and communicate key risk indicators (KRIs) and management activities to assist relevant stakeholders in their decision-making process.
- Facilitate independent risk assessments and risk management process reviews to ensure they are performed efficiently and effectively.
- Identify and report on risk, including compliance, to initiate corrective action and meet business

and regulatory requirements.

4. Information Systems Control Design and Implementation

Design and implement information systems controls in alignment with the organization's risk appetite and tolerance levels to support business objectives.

- Interview process owners and review process design documentation to gain an understanding of the business process objectives.
- Analyze and document business process objectives and design to identify required information systems controls.
- Design information systems controls in consultation with process owners to ensure alignment with business needs and objectives.
- Facilitate the identification of resources (e.g. people, infrastructure, information, architecture) required to implement and operate information systems controls at an optimal level.
- Monitor the information systems control design and implementation process to ensure that it is implemented effectively and within time, budget and scope.
- Provide progress reports on the implementation of information systems controls to inform stakeholders and to ensure that deviations are promptly addressed.
- Test information systems controls to verify effectiveness and efficiency prior to implementation.
- Implement information systems controls to mitigate risk.
- Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of information systems control performance in meeting business objectives.
- Assess and recommend tools to automate information systems control processes.
- Provide documentation and training to ensure information systems controls are effectively performed.
- Ensure all controls are assigned control owners to establish accountability.
- Establish control criteria to enable control life cycle management

5. Information Systems Control Monitoring and Maintenance

Monitor and maintain information systems controls to ensure they function effectively and efficiently.

- Plan, supervise and conduct testing to confirm continuous efficiency and effectiveness of information systems controls.
- Collect information and review documentation to identify information systems control deficiencies.
- Review information systems policies, standards and procedures to verify that they address the organization's internal and external requirements.
- Assess and recommend tools and techniques to automate information systems control verification processes.
- Evaluate the current state of information systems processes using a maturity model to identify the gaps between current and targeted process maturity.
- Determine the approach to correct information systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately considered and remediated.
- Maintain sufficient, adequate evidence to support conclusions on the existence and operating effectiveness of information systems controls.
- Provide information systems control status reporting to relevant stakeholders to enable informed decision making.

6. IT Policies/Governance and Compliance

- Coordinate the development and ongoing maintenance of other IT policies and procedures.
- Ensure that all IT policies and procedures are compliant with regulatory requirements.

- Maintain a schedule of policy review and submission to the board for approval

7. Disaster Recovery Coordination

- Maintain the IT Disaster Recovery Plan including annual reviews.
- Oversee the regular testing of the plan and update for major changes in hardware, applications, business and regulatory requirements accordingly.
- Coordinate testing and reporting of data backup restorations in accordance with Key Performance Indicators (KPIs).

8. Audits and Reviews Preparation and Facilitation

- Serve as liaison to auditors, consultants, and the bank Compliance Committee regarding documentation and review of information compliance.
- Communicate audit and review results to appropriate parties; ensure that issues are addressed and corrective actions are implemented.
- Keep a tracking action list of all audit issues.

9. Projects and Initiatives related to IT

- Participate in IT projects and initiatives to bring pro-active risk management focus into solutions.