IT Governance and Compliance Officer

COMPANY: SASFIN BANK LIMITED
DIVISION: Information Technology
DEPARTMENT: Information Security and Governance
JOB TITLE: IT Governance and Compliance Officer
MANAGER: Head of Information Security and Governance
LOCATION: Waverly, Johannesburg

MAIN PURPOSE OF THE JOB

IT Governance

The purpose of this role will be to support the Head: Information Security and Governance with all governance and control related functions. Responsible for ensuring that the respective functional heads have the correct IT policies, procedures, standards, RACI charts and practices for conformance with the IT Governance Framework and mandatory legislation and regulations, in place as defined by Group Compliance.

Taking into consideration the current maturity of IT as well as evolving needs of all stakeholders.

Work closely with IT Management team to establish and conduct oversight on Sasfin approach to the use of information and associated technologies, including the acceptance of responsibilities in respect of both supply of and demand for IT. Ensure that the respective accountable IT functional heads are providing input into the IT Dashboard and performance management reporting.

KEY AREAS OF RESPONSIBILITY

1. IT Governance
2. Information Governance
3. IT Governance Documentation – Policies, Standards, Processes and Procedures
4. IT Audit and Compliance Co-ordination

DESCRIPTION OF TASKS

1. Information Governance

1.1. Establish an information management and protection framework for an effective enterprise-wide Information Governance Program; serve as a consultant to business-area leaders
1.2. Identify, evaluate, and assist with the implementation of an information governance solution to provide systemic monitoring of the Information Governance program;
1.3. Manage day-to-day activities, including policies, procedures, training and communication regarding the Information Governance Program.
1.4. In conjunction with Group Legal and Group Compliance identify information management and protection laws and regulations and implement actions to ensure compliance.
1.5. Develop, implement and maintain the policies, systems, and procedures for the management of recorded information throughout its life cycle.

2. IT Governance

2.1. The purpose of this role will be to support the Head: Information Security and Governance with all governance and control related functions.
2.2. Ensuring that the respective functional heads have the correct IT policies, procedures, standards, and practices for conformance with the IT Governance Framework and mandatory legislation and regulations, in place, as defined by Group Compliance.
2.3. Define IT RACI charts defining the acceptance of responsibilities in respect of the supply and demand for IT.
2.4. Manage day-to-day activities related to developing and advising on the IT Functional Area development of governance documentation such as policies, standards, procedures and training.
2.5. Perform regular IT Governance Maturity Assessments for the respective IT Functional Areas.
2.6. Develop a training plan aligned to the IT Governance Program for all IT Functional Areas, based on the defined current Skills Matrix.

3. IT Governance Documentation

3.1. Manage of IT Governance policies, standards, processes and procedures. The development, enhancement, and maintenance across the documentation management lifecycle.
3.2. Exhibit broad knowledge of governance, compliance and auditing frameworks and apply that in reviewing the quality of existing and new documentation.
3.3. Recognize and identify potential areas where existing policies, standards and procedures require change.
3.4. Support additional internal and external compliance activity as part of the Information Security and Governance team
3.5. This position will work directly with technical and business leadership across the organization to select, deploy and validate security controls to ensure security and compliance requirements are maintained.
3.6. Subscribe to information security blogs and sector subscriptions to identify new risks and trends that may need to be address in information security policies, procedures and standards.

4. Implement IT Governance Risk and Compliance

Policy, Standards and Procedures:

Identify, evaluate, and assists with the implementation of an information governance archival solution to provide systemic monitoring of the Information Governance program; serve as a consultant to business-area leaders.

Departmental Compliance Officer

4.1. Ensure security programs are in compliance with relevant laws, regulations and policies to minimize or eliminate risk and audit finding, according the requirements defined by Group Compliance.
4.2. Ensure that IT staff understand their role in compliance.
4.3. Track and monitor IT Compliance initiatives.

5. IT Audit Management

5.1. Conducting internal assessments of IT Policies, Standards and Process compliance to IT Audit standards.
5.2. Manage relationships and interactions with internal and external auditors and risk management bodies, and reviewing and reporting on open issues both prior to and subsequent to issuance.
5.3. Discuss the IT Audit Plan.
5.4. Collaborate with Group IT to define audit scope.
5.5. Facilitate all requests for information from Group IT for audits.
5.6. Follow-up and provide feedback on all IT Audit findings by collaboration with IT Management.
5.7. Lead and manage the process of self-assessment as part of the overall IT Governance Framework.
5.8. Performs other related duties as required.

SKILLS AND QUALIFICATIONS REQUIRED

- A Bachelor's Degree in a related area such as; Computer Science or Information Technology.
- Risk-related industry-standard qualifications such as CISA, CISM or CGEIT would be a strong recommendation.
- Advantage will be COBIT, ISO2700X, and ITIL.
- Experience in compliance frameworks for Information Security, Compliance & IT Governance Standards: ISO27001, PCI-DSS, COBIT, King III
- Strong risk assessment/audit capabilities with hands on experience in many technologies and platforms across a broad range of industries.

PERSONAL ATTRIBUTES REQUIRED

Leadership

- Demonstrable integrity, empathy and emotional intelligence
- an influential leader with sound knowledge of business management
- working knowledge of information security technologies
- Proven ability to assess risks and controls and to identify solutions to reduce risk

Working Style

- The ability to collaborate across the organization with other teams, such as system operations, infrastructure, auditors and business users.
- Ability to design, evaluate and document processes and lead teams in accomplishing process review and improvement.

Communication Skills

- Ability to conduct governance, risk and compliance sessions
- Excellent written and verbal communications skills.
- Ability to feedback on governance, risk and compliance issues in a structured manner
- Demonstrated initiative and commitment for results and the ability to set priorities and manage multiple initiatives.
- Ability to adjust to changing priorities while multitasking effectively.
- Time Management
- Solid work ethic with attention to detail

- Ability to work under pressure

Conformance

- Strong process background in change control, backup strategies and disaster recovery
- Ability to adhere to very strict policies and procedures
- Focus on planning, testing and carefully controlled implementations

Excellent written/verbal/communication, listening and facilitation skills.

- Excellent time management and related organisational skills, including appropriate sense of urgency, a proactive approach, and a suitable ability to anticipate and manage project lifecycle events, issues and obstacles.
- Able to identify and document specific governance and compliance issues, propose resolution options, and interpret matters from the perspective of involved stakeholders.
- Consulting skills (client service orientation, conflict resolution, analysis/synthesis of information, negotiation, project management, presentation etc.)
- Negotiation skills needed to obtain commitments to remediate risks from leadership of other teams.
- Ability to work on own initiative.

REMUNERATION

Market-related, based on total Cost to Company

Interested applicants can forward their CV to sasfinrecruitment@sasfin.com by no later than: 07 April 2015.

*Please consider your application unsuccessful if you have not received a response within 2 weeks of submission.