JOB DESCRIPTION

Position Summary/Overview:
The IT Manager's role is to plan, coordinate, direct, and design operational activities of the IT Department, as well as provide direction and support for IT solutions that enhance mission-critical business operations. The IT Manager ensures the streamlined operation of the IT Department in alignment with the business objectives of the organization. This individual will collaborate directly with the management team and decision makers in other departments to identify, recommend, develop, implement, and support cost-effective technology solutions for all aspects of the organization. This person will also develop and implement IT policies, procedures, risk assessments, and best practices.

Functions / Responsibilities*

Strategy & Planning

- Participate in strategic and operational governance of policies and processes of the organization.
- Lead IT strategic and operational planning to achieve business goals by fostering innovation, prioritizing IT initiatives, and coordinating the evaluation, deployment, and management of current and future IT systems and products.
- Make recommendations for the improvement and growth of the IT infrastructure and IT systems.
- Develop business case justifications and cost/benefit analyses for IT spending and initiatives.
- Assist the ISO develop an annual project and support budget
- Assist the ISO develop and maintain an appropriate IT organizational structure that supports the needs of the business.
- Assist the ISO negotiate and administer vendor, outsourcer, and consultant contracts and service agreements.
- Assist the ISO review hardware and software acquisition and maintenance contracts and pursue master agreements to capitalize on economies of scale.
- Keep current with trends and issues in the IT industry, including current technologies and prices.
- Supervise IT staff in accordance with corporate budgetary objectives and personnel policies.

Operational Management

- Establish IT departmental goals, objectives, and operating procedures.
- Act as an IT advocate via regular written and in-person communications with the department managers and end users.
- Develop business case justifications, cost/benefit analyses, assess and communicate risks associated with initiatives.
- Coordinate and facilitate consultation with ISO and Co-Chair the IT steering committee to define business and systems requirements for new technology implementations. Conduct a minimum of quarterly ITSC meetings annually.
- Ensure continuous delivery of IT services through oversight of service level agreements with end users and monitoring of IT systems performance.
- Assist the ISO define and communicate corporate plans, policies, and standards for the organization for acquiring, implementing, and operating IT systems.
- Assist the ISO prioritize, and control projects and the project portfolio as they relate to the selection, acquisition, development, and installation of major information systems.

- Oversee, Track and maintain all software/hardware changes, upgrades, etc on the Change Management Tracking Log. Ensure time lines and due dates are met as required. Report ongoing results and progress to the ITSC.
- Corodata Offsite Storage Management including managing users, ordering boxes, updating logs, inventory control, and destruction of boxes. Also, maintaining and updating procedures.

Regulatory/Consumer Compliance Responsibilities

- Ensure IT policies and system operations adheres to applicable laws and regulations.
- Act as the primary contact for regulatory IT examinations and auditors.
- Maintain knowledge regarding Information Security related Policies and procedures. This includes knowledge of the Gramm-Leach-Bliley Act / GLBA 501 (b), Information Security Program rules, Red Flags and internal GLBA Privacy Policy.
- Conduct ongoing information security risk assessments and data classification
- Maintain documentation of exceptions to information security policies and procedures or regulatory requirements
- Assist in new product, system or service implementation to ensure all information security related risks have been identified and compensating controls have been implemented
- Maintain a comprehensive Information Security Program
- Assist in the creation and review of the Information Technology Policy as it pertains to the information security function
- A working knowledge of the Bank's BSA Policy and procedures as it relates to operational procedures, deposit products and services. This includes the regulations regarding the BSA, USA Patriot Act, OFAC and Anti-Money Laundering which are collectively referred to as the BSA. Suspicious Activity Reporting through the Bank's internal procedure is expected to be understood and utilized when needed. A working knowledge of the Bank's Customer Identification Program and Currency Transaction Reporting system and teller – line procedures is required. Further, High Risk Customer procedures, Customer Identification Program and other account and transaction related BSA policy duties is required. Confidentiality of all BSA policy, procedures and customer transactions or activity is essential.
- Responsible for maintaining knowledge of compliance related laws, policies, procedures and duties to ensure consumer privacy and protections.
- Responsible to maintain knowledge of Fair Lending and the Community Reinvestment Act to promote fair and equal treatment, policy and product development with the loan policy and other related services and strategies for the Bank.
- Maintain an understanding of the Bank's Complaint Policy and reporting procedure. Must have knowledge of the Bank's Anti-Harassment Policy, Code of Conduct and protocols if issues arise.
- Accountable for the timely completion all assigned online Computer Based Training courses. Participate in conferences, webinars or other training opportunities as recommended by the ISO and/or Compliance Officer.
- Participate in compliance related training opportunities as recommended by the position supervisor.

Implementation

- Develop and maintain an information systems security control framework
- Manage the information security function to meet organizational requirements
- Maintain familiarity with a variety of IT security concepts, practices, and procedures

- Ensure all applications and systems are secure
- Ensure the safeguarding of all customer non-private personal information
- Establish safe procedures for review and approval and verification of user application and systems access requests

Oversight, monitoring, and awareness

- Ensure compliance with IT security standards and existing policies and procedures
- Establish procedures and automated processes for monitoring information systems
- Identify applicable cyber threats (e.g., zero day vulnerabilities) and develop remediation strategies
- Represent the information security function on the IT Committee and periodically update the IT Committee and the Board regarding the status of the information security function
- Prepare and present the annual report on the status of the Information Security Program to the Board
- Coordinate with internal audit to ensure testing of the information security area and assist the organization with special projects and audits as needed
- Complete any assigned corrective action as needed and submit completed Remediation reports to the MCC for review and verification.
- Implement information security awareness, training, and educational activities for all employees and Management. Report results to the ITSC quarterly.
- Ensure users are given only the appropriate access needed for their functions

Incident management

- Direct development and execution of an enterprise-wide BCP and disaster recovery plan.
- Provide and coordinate the annual disaster recovery testing design and implementation.
- Establish and maintain a comprehensive Incident Response Plan
- Investigate security breaches and assist with any associated disciplinary and legal matters
- Maintain sufficient documentation regarding identified information security issues and the steps taken for correction, risk transfer, or risk acceptance
- Respond to information security breaches and notify clients, the public, law enforcement and regulatory bodies, as applicable
- Report all information security breaches to the BSA Officer for applicable SAR filing

Primary Location
South San Francisco, CA

Other Locations
Boulder Creek, CA; Felton, CA

Travel
Yes, 10% of the Time

Average Hours Per Week
40 hrs

Days per week
Monday through Friday, some weekends as necessary
On Call is required (Cell phone issued)

Environment:

Physical Demands:

The physical demands described are representative of those that must be met by an employee to successfully perform the essential functions of this position. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Office Environment:

While performing the duties of this job, the employee is regularly to sit for one or more continuous hours; and/or stand for one or more continuous hours. The employee frequently is required to use hands to finger motions and reach with hands and arms, stoop or crouch.

The employee must occasionally lift and move up to 25 pounds. Specific vision abilities required by this position include close vision and the ability to adjust focus.

***Note:** This job description is not intended to be all-inclusive. Employee may perform other related duties as assigned to meet the ongoing needs of the organization. Job duties and supervisor reporting relationship may change.