Roles scenario essay sample

Finance

1. The relationship between fiduciary responsibility and organizational risk, from an IT position begins with acting on behalf of YieldMore is to performs risk analysis, identifying and assessing factors that may jeopardize the success of a project or achieving a goal. The fiduciary can use one of the more popular risk analysis methods called Facilitated Risk Analysis Process (FRAP) which will analyze one system, application or segment of business process at a time. By executing the two primary principles of “ due diligence”, and “ due care”, the fiduciary has an obligation to not only identify all possible organizational risks but to identify controls which could mitigate the risk.

2. The stakeholders within YieldMore are the CEO who has overall control of the company to the production team who ensures the product is deployed according to established timetables, sales team who tracks customers and is in charge of advertisement, quality control team which makes sure the product meets standards of the company, finance team which oversees not only sales but company salaries, company assets and liabilities, and last but not least, the IT management team which manages the servers, workstations, applications and entire network infrastructure.

3. The fiduciary is responsible for providing the CEO with a comprehensive risk analysis plan that addresses the identified risks in each department. For example the finance department must have a separation of duties policy so that no one person has control over, say the payroll of employees. Ensure that the company’s proprietory database software and intellectual property is protected from data loss and that there is a disaster recovery plan and all members of YieldMore are aware of there is an acceptable use policy.

4. Fiduciaries through their actions, or inactions, motivated by malice, or through ignorance or neglect, may be held personally liable if they breach their duties. One way to reduce the risk of being held personally liable is to establish a compliance procedure. Once compliance procedures are established follow them precisely, documenting the process and the decisions made along the way. 5. The following is a brief report by the IT management team identifying the organizational risks and controls which could mitigate these risks: RISK/VULNERABILITY

MITIGATION

Fire

Install and maintain fire suppression system

Hurricane, earthquake, tornado, flood

Develop and test disaster recovery plan

Malware

Install anti-virus software, update AV definitions weekly, Acceptable use policy Equipment failure

Backup data daily/weekly

Network instrusion

Install IDS, monitor network traffic

Stolen data

Access controls, separation of duty, least user privilege controls

Unauthorized access to DB files

Enforce access controls, separation of duty, least user privilege controls

Unauthorized remote access

Install VPN tunneling procedures and access controls