Most organizations rely significantly upon information and communication technology and the internet in their day to day operations. Irrespective of size and type, they need a suitable set of information security controls and related security management practices to ensure that their systems and data are appropriately protected against security threats. This study investigated the current state of information systems security controls and related security management practices in small and medium enterprises in the financial sector particularly SME banks and how ISO 27002 can be implemented successfully based on ISO 27001 standard to maintain an effective information security management system that ensures confidentiality, integrity and availability of information. The population of study constituted -37 small and medium size banks in Kenya classified according to the weighted composite index by the Central Bank of Kenya. A descriptive survey design was used in this study because it mostly involved the use of non-numerical data of descriptive nature. Stratified sampling was used to create a sampling frame for the SME banks. A sample size of 33.3% out of the accessible target population of 37 SME banks in Kenya was used which gave 8 small size banks and 5 medium size banks totaling to 13 SME banks in Kenya who have operations in Kisumu City CBD where the study was conducted. 4 respondents were randomly picked from each sampled institution using purposive sampling giving a total of 52 respondents. 41 questionnaires were received representing a response rate of 78.9%. Data analysis was clone using SPSS version 16. Primary data collected was analyzed using descriptive statistics which were tabulated and presented in pie charts and graphs. The findings of this study established that information security controls in SMEs are insufficient to deal with information security threats and malpractices clue to lack of: information security education, training and awareness programs; regular and periodic reviews; policy enforcement; and resources. These deficiencies have been highlighted and appropriate preventive and corrective measures such as: education training and awareness programs; regular and periodic information security reviews and audits; policy enforcement; adequate internal and identity controls; and proper risk assessment recommended for continual information systems security. The findings of this study will enable organization heads to request for an increased budget for information security implementation within a certain budget.