Control # Reference	Finding #	Finding Heading	Finding Description

Finding Rating	Finding Impact	Recommendations

Compliance References

Domain	Control Objective	Control #
Security policy	Information security policy	Information security policy document
Security policy	Information security policy	Review of the information security policy
Organizational of information security	Internal organization To manage information security within the organization	Management commitment to information security

Questions
1,2,3,4,5,6,7,8,9
10,11,12,13,14
3,6,8,14

Question Number	Tags	Question Text
1	ISO27001, ISO20000	Is there a written policy document which is approved by the management?
2	PCIDSS, ISO27001	Is policy document available to all employees responsible for information security?
3	ISO20000, PCIDSS	Does the policy contain a definition of information security - its overall objectives and scope, and its importance as an enabling mechanism for information sharing?
4	ISO 9000,ISO 14000, ISO 22000	Does the policy contain a statement of management intention supporting the goals and principles of information security?
5	ISO 9000,ISO 14000, ISO27001	Does the policy contain a definition of general management responsibilities and specific Company responsibilities for all aspects of information security?
6	ISO27001	Does the policy contain an explanation of security polices, principles, standards and compliance requirements, including the following? - compliance with legislative, regulatory, and contractual requirements - security education, training, and awareness requirements - business continuity management - consequences of information security policy violations
7	PCIDSS	Does the policy contain an explanation of the process for reporting of suspected security incidents?
8	ISO20000	Does the policy contain references to documentation which may support the policy?
9	ISO9000	How is the policy communicated to the users?
10	ISO22000	Does the policy have a clear owner?
11	ISO 9000,ISO 14000, ISO27001	Is there a defined review process, including responsibilities and schedule for review?
12	ISO 9000,ISO 14000, ISO27001	Does the review embrace the effectiveness of the policy, changes to the organizational environment, business circumstances, legal conditions and technical environment?
13	ISO 9000,ISO 14000, ISO27001	Are the policy documents updated according to defined schedule?
14	ISO 9000,ISO 14000, ISO27001	Is revised policy approved by management?
15	ISO 9000,ISO 14000, ISO27001	Does a high level information security steering forum exist, to give management direction and support?
16	ISO 9000,ISO 14000, ISO27001	Are information security responsibilities explicitly assigned and acknowledged?

17	ISO 9000,ISO 14000, ISO27001	Are the following addressed by the information security steering forum? - Identification of information security goals - Formulation, Review and approval of information security Policy - Review the effectiveness of the implementation of the information security policy - Provisioning resources required for information security - Approving assignment of specific roles and responsibilities for information security across the organization - Approval of Security Initiatives - Ensuring implementation of information security controls being coordinated across the organization - Initiating plans and programs to maintain information security awareness