7.3 Organizational perspectives and groups

7.3.1 Policy

Rate as Yes or No. Count Yes answers and divide by 2 for a total (out of 10).

Area	*Issue*	*Rate*
Governance	Policy defines who is in charge of protection issues.	
	Policy identifies other standard and procedure documents.	
	Policy defines the structure of who is in charge of what.	
Align w/value	Policy asserts protection as commensurate with value.	
	Policy defines how risk thresholds are determined.	
	Policy defines security architectural requirements	
Power	Power issues are codified in policy by granting individuals and groups control over resources and actions.	
	Information protection has adequate power under policy.	
	The CISO function has the right of covert inspection.	
	The CISO reports on protection to the CEO or board.	
Feedback	Feedback mechanisms are provided via policy.	
	Audit provides feedback to the CISO function by policy.	
	The CISO has the right of inspection for feedback.	
Budget	Adequate budget is provided to the CISO for the function.	
	The budget process assures ongoing adequate funding.	
Appeals	Appeals processes are define under policy.	
	The CISO has a strong position in the appeals process.	
Acceptable use	Acceptable use policy identifies what is and is not allowed in the use of enterprise resources.	
Obey laws	Obeying laws is codified in policy.	
	Adequate knowledge and awareness of laws is provided.	
TOTAL	Add the number of Yes answers and divide by 2.	
Rating	Multiply TOTAL by the likelihood that policies are followed.	

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
2.5	7	8	9	9.5