

7.3.2.5 COSO rating

COSO is the regulatory mandated risk management framework for Sarbanes-Oxley review. The COSO cube provides an overview of COSO requirements.



7.3.2.6 The COSO Cube

For each white area, rate the mix from 0 to 10 (e.g., {Strategic x Entity x Monitor} rates how well the strategic entity security vision is realized in program monitoring). Under R (blue), sum each row and divide by 7. Sum columns and divide by 16 in the yellow areas. Sum category entries / 28 in the green areas. Add the blue areas / 4 plus the green areas plus the yellow areas, divide by 15, and enter the overall rating.

Category	Level	Set objectives	Identify events	Assess Risks	Respond to risks	Control activities	Comm - unicate	Monitor	R
Strategic	Entity								
	S=sum/28	Division							
		Bus-Unit							
		Subsidiary							
Operations	Entity								
	O=sum/28	Division							
		Bus-Unit							
		Subsidiary							
Reporting	Entity								
	R=sum/28	Division							
		Bus-Unit							
		Subsidiary							
Compliance	Entity								
	C=sum/28	Division							
		Bus-Unit							
		Subsidiary							
Total	(sum / 16)								

Overall rating =

Startup	Diligence	Typical	Excellent	Best
0	7.5	5	8	9