7.3.2.8 Standards roll-up

Determine which standards are desirable for the enterprise and then use the standard-specific rating system, determine ratings. Fill in the rating and goal for each applicable standard and identify the desired standards by entering Yes in the applicable boxes. Add up the ratings, divide the rating by the goal state and generate an overall rating for standards.

Standard	*Issue*	*Rate*	*Goal*
GAISP	GAISP and/or GASSP are followed as defined enterprise information protection control standards.		
	Enter the GAISP roll-up ratings for current and desired.		
ISO17799	ISO17799 is used for policy development.		
	Enter the ISO 17799 ratings for current and desired.		
CMM-SEC	CMM-SEC is used as a key measurement of program performance and goal are set for achieving and maintaining a suitable level for the enterprise as part of the program.		
	Enter the CMM-SEC ratings for current and desired.		
COBIT	COBIT is followed as a control standard.		
	Enter the CoBit ratings for current and desired.		
COSO	COSO is followed as a control standard.		
	Enter the COSO ratings for current and desired.		
CISWG	CISWG is followed as a control standard.		
	Enter the CISWG ratings for current and desired.		
Technical	Technical standards for information protection are used when applicable.		
TOTAL	Add ratings/(10 *number of standards applied).		
Rating	Divide the rating by the goal and multiply by 10		70

Expressed as total /7:

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
1.9	5	7	8.5	9.75

A reasonable goal for the metric would be 40 for a top flight enterprise, choosing between CoBit and ISO 17799 as the preferred standard. Goals below 20 are likely less than would be mandated by minimums of due diligence.