Building an ISO 27001-Compliant Cybersecurity Program: Getting Started

with Marc Menninger

LEARNING

Risk Register

Risk Treatment M = Risk Reduction/Mitigation A = Risk Acceptance Av = Risk Avoidance T = Risk Transfer							Risk Score = Impact x Likelihood Residual Risk = Risk That Remains after Controls (Risk Treatment) Have Been Implemented				
Impact Description (The Business Consequences of a Successful Exploit)	Risk Owner	Confidentiality (L,M,H)	Integrity (L,M,H)	Availability (L,M,H)	Impact (1–3)	Likelihood (1–3)	Risk Score (1–9)	Risk Treatment Required (Y/N)	Risk Treatment (M, A, Av, T)	Residual Risk (1–9)	Residual Risk Accepted

Risk Level Matrix				
Impact	Catastrophic (3)	Low (3)	Medium (6)	High (9)
	Moderate (2)	Low (2)	Medium (6)	Medium (6)
	Minor (1)	Low (1)	Low (2)	Low (3)
		Unlikely (1)	Possible (2)	Likely (3)
	Likelihood			

Risk Treatment Recommendations		
Risk Treatment	**Risk Treatment Definition**	**Key**
Risk reduction/ mitigation	The level of risk should be reduced through the selection of controls so that the residual risk can be re-assessed as being acceptable.	M
Risk acceptance	If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls, and the risk can be retained.	A
Risk avoidance	The activity or condition that gives rise to the particular risk should be avoided by withdrawing from an activity or changing the conditions under which the activity is operated.	Av
Risk transfer	Transfer the risk to another entity (such as by contract or insurance).	T