Self Assessment mit Standardfragebogen und GAP-Analyse

1 Standardisierter Fragebogen

- Ermittlung des Status Quo
- Analyse der vorhandenen relevanten Dokumentationen, Richtlinien und sonstigen Regelwerken
- Erhebung des fachlichen Ist-Zustands mittels strukturierten Interviews, Fragebögen und Workshops
- Validierung des Status Quo auf Basis der wesentlichen ISO 27001 Anforderungen

Srl	M	Assement Objective	Audit Tests	Findings	Compliance	Status	Remarks
Security Policy 1							
1.1		Roles, Accountability and Responsibilities			65.00%	At Risk	
1.1.1	1	Identify board level representative responsible for security	sddasd	There is no responsible for security.	75.00%	Near Compliant	
1.1.2	1	Identify designated SIRO			100.00%	Compliant	
1.1.3	1	Ensure SIRO responsibilities include management of organisation's information risks.			50.00%	At Risk	
1.1.4	1	Ensure the Information Risk Register is properly maintained.			0.00%	Non-Compliant	
1.1.5	1	Identify designated DSO.			100.00%	Compliant	
1.1.6	1	Ensure DSO day to day responsibilities cover all aspects of Protective Security.					
1.1.7	1	Review requirements for specialist security roles.					
1.1.8	1	Review documentation detailing security					
1.1.9	1	Ensure all individuals with designated security responsibilities have appropriate training for the					
1.2		Security Risk Management					
1.2.1	2	Adopt an organisation-wide holistic risk management approach to rotective security which is aligned to HMT Orange Book principles.					
1.2.2	2	Develop local security policies tailored to relevant business needs, threat profiles and risk appetite.					
1.2.3	2	Maintain a Protective Security Risk Register.					
1.3		Culture, Education and Awareness					
1.3.1	3	Ensure all staff are provided with guidance regarding relevant legislation (DSA, DPA, FOIA etc).					
1.3.2	3	Ensure staff handling PMM are given specific guidance on how legislation relates to their role.					
1.3.3	3	Ensure Security awareness & education is built into staff induction.					
1.3.4	3	Ensure all staff complete regular security					
1.3.5	3	Ensure there are demonstrable plans to foster a culture of proportionate protective security.					
1.3.6	3	Ensure all users of ICT systems are familiar with SyOPS and have received appropriate security training for their use.					

2 GAP-Analyse und grafische Auswertung

- Gap-Analyse mit Bewertung und Priorisierung auf fachlicher, organisatorischer und prozessualer und technischer Ebene
- Ableitung von high-level Handlungsbedarfen
- Strukturierte Dokumentation aller Ergebnisse

GAP-Analyse - Benchmark zu ISO 27001