PGM CONSULTING

ISO 27001 GAP ANALYSIS / AUDITS

Assessment 2024

Client:
Date:

Requirement	Requirement	Status	Compliance (Yes, No)	Evidence	Addit. Info
4 Context of the organisation		40%			
4.1 Policies for information security	Have the internal and external issues that are relevant to the ISMS, and that impact on the achievement of its expected outcome, been determined?		No		
4.2 Understanding the needs and Expectations of interested parties	Has the organisation determined the interested parties that are relevant to the ISMS?	40%	No	Necessita de ser clarificado as necessidades e expetativas que temos em termos de SI.	
4.2 Understanding the needs and Expectations of interested parties	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?	40%	No		Weak . A inexistência de um elemento de cibersecuranga global para a Org.
4.3 Scope of the isms	Have the boundaries and applicability of the ISMS been determined to establish its scope, taking into consideration the external and internal issues, the requirements of interested parties and the interfaces and dependencies with other organizations?	...	N/A		OM - revisão
4.3 Scope of the isms	Is the scope of the ISMS documented?	...	N/A		
5 Leadership		70%			
5.1 Leadership and commitment	Does Top Management demonstrate leadership and commitment in establishing the information security policy and objectives, in consideration of the strategic direction of the organization, and in promotion of continual improvement?	...	N/A		
5.1 Leadership and commitment	Does Top Management demonstrate leadership and commitment in ensuring the integration of the ISMS requirements into its business processes?	70%	Yes		
5.1 Leadership and commitment	Does Top Management demonstrate leadership and commitment in ensuring that resources are available for the ISMS, and directing and supporting individuals, including management, who contribute to its effectiveness?	...	N/A		
5.1 Leadership and commitment	Does Top Management demonstrate leadership and commitment in communicating the importance of effective information security and conformance to ISMS requirements?	...	N/A		
5.2 Policy	Is there an established information security policy that is appropriate, gives a framework for setting objectives, and demonstrates commitment to meeting requirements and for continual improvement?	...	N/A		
5.2 Policy	Is the policy documented and communicated to employees and relevant interested parties?	...	N/A		
5.3 Organizational roles, responsibilities and authorites	Are the roles within the ISMS clearly defined and communicated?	...	N/A		
5.3 Organizational roles, responsibilities and authorites	Are the responsibilities and authorities for conformance and reporting on ISMS performance assigned?	...	N/A		
6 Planning		28%			
6.1 Address risk and opportunities	Have the internal and external issues, and the requirements of interested parties been considered to determine the risks and opportunities that need to be addressed to ensure that the ISMS achieves its outcome, that undesired effects are prevented or reduced, and that continual improvement is achieved?	20%	No	NC - Não foi envidência a identificação de Riscos e Oportunidades, via Analise SWOT para a Segurança de Informação.	Prevista ser realizada em Janeiro 2025.
6.1 Address risk and opportunities	Have actions to address risks and opportunities been planned, and integrated into the ISMS processes, and are they evaluated for effectiveness?	20%	No		
6.1.3 Information security risk treatment	Is there an information security risk treatment process to select appropriate risk treatment options for the results of the information security risk assessment, and are controls determined to implement the risk treatment option chosen?	100%	Yes	P 02 4 30 - Risk Assessment Procedure	
6.1.3 Information security risk treatment	Have the controls determined, been compared with ISO/IEC 27001 Annex A to verify that no necessary controls have been missed?	10%	No	Não Foi ainda definido	
6.1.3 Information security risk treatment	Has a Statement of Applicability been produced to justify Annex A exclusions, and inclusions together with the control implementation status?	10%	No	Não Foi ainda definido	
6.1.3 Information security risk treatment	Has an information security risk treatment plan been formulated and approved by risk owners, and have residual information security risks been authorised by risk owners?	10%	No	Thats will be aproved in tha System Review meeting	
6.1.3 Information security risk treatment	Is documented information about the information security risk treatment process available?	...	N/A		
6.2 Information security objectives and planning to achieve them	Have measurable ISMS objectives and targets been established, documented and communicated throughout the organization?	...	N/A		it is not defined the protection time for the relevant records
6.2 Information security objectives and planning to achieve them	In setting its objectives, has the organization determined what needs to be done, when and by whom?	...	N/A		
7 Support		60%			
7.1 Resources	Is the ISMS adequately resourced?	...	N/A		
7.2 Competence	Is there a process defined and documented for determining competence for ISMS roles?	...	N/A		
7.2 Competence	Are those undertaking ISMS roles competent, and is this competence documented appropriately?	60%	Yes	Job Description - 2024-02-18	It was not defined some critical job profiles or responsabilities. Ex. ISMS Manager,
7.3 Awareness	Is everyone within the organization's control aware of the importance of the information security policy, their contribution to the effectiveness of the ISMS and the implications of not conforming?	...	N/A		
7.4 Communication	Has the organization determined the need for internal and external communications relevant to the ISMS, including what to communicate, when, with whom, and who by, and the processes by which this is achieved?	...	N/A		
7.5 Documented information	Has the organization determined the documented information	...	N/A		

PGM CONSULTING

ISO 27001 GAP ANALYSIS / AUDITS

Assessment 2024

Client:
Date:

Requirement	Requirement	Status	Compliance (Yes, No)	Evidence	Addit. Info
7.5 Documented information	Is the documented information in the appropriate format, and has it been identified, reviewed and approved for suitability?	...	N/A		
7.5 Documented information	Is the documented information controlled such that it is available and adequately protected, distributed, stored, retained and under change control, including documents of external origin required by the organization for the ISMS?	...	N/A		
8 Operations		70%			
8.1 Operational planning and control	Has a programme to ensure the ISMS achieves its outcomes, requirements and objectives been developed and implemented?	...	N/A		
8.1 Operational planning and control	Is documented evidence retained to demonstrate that processes have been carried out as planned?	70%	Yes		
8.1 Operational planning and control	Have outsourced processes been determined and are they controlled?	...	N/A		
8.1 Operational planning and control	Are information security risk assessments performed at planned intervals or when significant changes occur, and is documented information retained?	...	N/A		
8.1 Operational planning and control	Has the information security risk treatment plan been implemented and documented information retained?	...	N/A		
9 Performance evaluation		40%			
9.1 Monitoring, measurement, analysis and evaluation	Is the information security performance and effectiveness of the ISMS evaluated?	40%	No		
9.1 Monitoring, measurement, analysis and evaluation	Has it been determined what needs to be monitored and measured, when, by whom, the methods to be used, and when the results will be evaluated?	...	N/A		
9.1 Monitoring, measurement, analysis and evaluation	Is documented information retained as evidence of the results of monitoring and measurement?	...	N/A		
9.2 Internal audit	Are internal audits conducted periodically to check that the ISMS is effective and conforms to both ISO/ IEC 27001 and the organization's requirements?	...	N/A		
9.2 Internal audit	Are the audits conducted by an appropriate method and in line with an audit programme based on the results of risk assessments and previous audits?	...	N/A		
9.2 Internal audit	Are results of audits reported to management, and is documented information about the audit programme and audit results retained?	...	N/A		
9.2 Internal audit	Where non conformities are identified, are they subject to corrective action?	...	N/A		
9.3 Management review	Do top management undertake a periodic review of the ISMS?	...	N/A		
9.3 Management review	Does the output from the ISMS management review identify changes and improvements?	...	N/A		
9.3 Management review	Are the results of the management review documented, acted upon and communicated to interested parties as appropriate?	...	N/A		
10 Improvement		20%			
10.1 Nonconformity and corrective action	Have actions to control, correct and deal with the consequences of non-conformities been identified?	...	N/A		
10.1 Nonconformity and corrective action	Has the need for action been evaluated to eliminate the root cause of non-conformities to prevent reoccurrence?	20%	No		
10.1 Nonconformity and corrective action	Have any actions identified been implemented and reviewed for effectiveness and given rise to improvements to the ISMS?	...	N/A		
10.1 Nonconformity and corrective action	Is documented information retained as evidence of the nature of non-conformities, actions taken and the results?	...	N/A		