7.3.2.2 GAISP rating

Ratings are given as **Poor**, **Fair**, or **Good** indicating the extent to which compliance was observed. Rate each area in terms of goals and do an assessment to determine current ratings. Add up ratings giving 0 for poor, 1 for fair, and 2 for good and divide by 4.6 to get summary ratings.

Area of the GAISP	*Rate*	*Goal*
2.1.1 Accountability Principle: Information security accountability and responsibility are clearly defined and acknowledged.		
2.1.2 Awareness Principle: All parties, including but not limited to information owners and information security practitioners, with a need to know have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and are informed of applicable threats to the security of information.		
2.1.3 Ethics Principle: Information is used, and the administration of information security is executed, in an ethical manner.		
2.1.4 Multidisciplinary Principle: Principles, standards, conventions, and mechanisms for the security of information and information systems address the considerations and viewpoints of all interested parties.		
2.1.5 Proportionality Principle: Information security controls are proportionate to the risks of modification, denial of use, or disclosure of the information.		
2.1.6 Integration Principle: Principles, standards, conventions, and mechanisms for the security of information are coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.		
2.1.7 Timeliness Principle: All accountable parties act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems.		
2.1.8 Assessment Principle: The risks to information and information systems is assessed periodically.		
2.1.9 Equity Principle: Management respects the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.		
2.2.1 Information Security Policy: Management ensures that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Such guidance assigns responsibility, the level of discretion, and how much risk each individual or organizational entity is authorized to assume.		

Area of the GAISP	*Rate*	*Goal*
2.2.2 Education and Awareness: Management communicates information security policy to all personnel and ensure that all are appropriately aware. Education includes standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences.		
2.2.3 Accountability: Management holds all parties accountable for their access to and use of information, e.g., additions, modifications, copying and deletions, and supporting Information Technology resources. It is possible to affix the date, time, and responsibility, to the level of an individual, for all significant events.		
2.2.4 Information Management: Management routinely catalogs and values information assets, and assigns levels of sensitivity and criticality. Information, as an asset, is uniquely identified and responsibility for it assigned.		
2.2.5 Environmental Management: Management is considered and compensates for the risks inherent to the internal and external physical environment where information assets and supporting Information Technology resources and assets are stored, transmitted, or used.		
2.2.6 Personnel Qualifications: Management establishes and verifies the qualifications related to integrity, need-to-know, and technical competence of all parties provided access to information assets or supporting Information Technology resources.		
2.2.7 System Integrity: Management ensures that all properties of systems and applications that are essential to or relied upon to support the organization's mission are established, preserved, and safeguarded.		
2.2.8 Information Systems Life Cycle: Management ensures that security is addressed at all stages of the system life cycle.		
2.2.9 Access Control: Management establishes appropriate controls to balance access to information assets and supporting Information Technology resources against the risk.		
2.2.10 Operational Continuity and Contingency Planning: Management plans for and operates Information Technology in such a way as to preserve the continuity of organizational operations.		
2.2.11 Information Risk Management: Management ensures that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable.		
2.2.12 Network and Infrastructure Security: Management considers the potential impact on the shared global infrastructure, e.g., the Internet, public switched networks, and other connected systems when establishing network security measures.		

Area of the GAISP	*Rate*	*Goal*
2.2.13 Legal, Regulatory, and Contractual Requirements of Information Security: Management takes steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.		
2.2.14 Ethical Practices: Management respects the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.		

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2.5	5	7	9	10

The total goal for GAISP compliance should be 10 for all enterprises. There is nothing in the GAISP that is not desirable for efficient and effective operations of information protection. Due diligence level is a 5 with nothing below a rating of Fair. The excellent level is rarely reached because it is hard to be good at everything. Ratings of fair are acceptable, and many of the more detailed issues take priority over the strategic level efforts associated with GAISP. As information protection programs mature they tend to get closer to the 10 level.