|  |  |
| --- | --- |
| ISO 27001 Information Security Management System | |
|  | |
| 11/27/2020 | Duc Phu Pham |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | ISO 27001The goal of ISO 27001 is to provide a framework of standards for how a modern organization should manage their information and data. Risk management is a key part of ISO 27001, ensuring that the organization understands where their strengths and weaknesses lie. ISO maturity is a sign of a secure, reliable organization which can be trusted with data.The International Organization for Standardization (ISO) has developed the ISO 27001 Standard to be widely applicable for many purposes, including:To assist organizations in formulating information security requirements and objectives.To assist organizations in ensuring that security risks are cost effectively managed.To assist organizations in complying with laws and regulations.To provide organizations with a process framework for the implementation and management of controls to meet security objectives.To assist in the definition of new information security management processes.To assist in the identification and clarification of existing information security management processes.For use by Management of organizations to determine the status of information security management activities.For use by internal and external auditors of organizations to determine the degree of compliance with Information Security policies, directives and standards adopted by an organization.For use by organizations in providing relevant information about information security to internal and external stakeholders.Benefit of ISO 27001Allows for the secure exchange of information This standard helps you identify the threats toward your information security and create plans to address them. Helps you identify the threats toward your information security and create plans to address them When you implement ISO 27001 in your company, you create awareness among employees and provide information security training to allow them to become accountable for information security, regardless of their role in the organization. Brings a competitive advantage and builds reputation Having certification to an information security standard such as ISO 27001 is a strong way of demonstrating that you care about your partners and clients’ assets as well. Meets legal or third-party obligations This standard is recognized and used by many organizations worldwide, and by applying its clear and practical instructions, you can prove your trustworthiness concerning information and data security. Achieve a return on investment By implementing this standard, you can achieve a return on investment in at least two ways. One way is through the marketing value that it adds to your organization since the certification can attract potential clients and also assist with pre-sales due diligence conducted by your potential clients.  Second, ISO 27001 helps you avoid, eliminate, or reduce the undesired effect of risks which otherwise can severely impact your organization’s reputation leading to financial penalties and related legal issues. Recommendation To comply with HIPPA Security Rules, the organization needs to satisfy three type of safeguards:   1. Administrative Safeguards   Administrative safeguards are the policies and procedures that help protect against a breach. They determine documentation processes, roles and responsibilities, training requirements, data maintenance policies and more. Administrative protections ensure that the physical and technical protections are implemented properly and consistently.   1. Physical Safeguards   Physical safeguards make sure data is physically protected. They include security systems and video surveillance, mobile devise, door and window locks, and locations of servers and computers.   1. Technical Safeguards   Technical safeguards are the technology and related policies that protect data from unauthorized access. Each covered entity needs to determine which technical safeguards are necessary and appropriate for the organization in order to protect its ePHI. | |  |
|  | 1. Annex A.5 – Information security policies This annex is designed to make sure that policies are written and reviewed in line with the overall direction of the organization’s information security practices. 2. Annex A.17 – Information security aspects of business continuity management The aim of Annex A.17 is to create an effective system to manage business disruptions.  Its divided into two sections. Annex A.17.1 addresses information security continuity – outlining the measures that can be taken to ensure that information security continuity is embedded in the organization’s business continuity management system.  Annex A.17.2 looks at redundancies, ensuring the availability of information processing facilities. | |  |
|  |
|  | 5. Annex A.13 – Communications security This annex concerns the way organizations protect information in networks.  It is divided into two sections. Annex A.13.1 concerns network security management, ensuring that the confidentiality, integrity, and availability of information in those networks remains intact.  Meanwhile, Annex A.13.2 deals with the security of information in transit, whether it is going to a different part of the organization, a third party, a customer or another interested party. 3. Annex A.10 – Cryptography This annex is about data encryption and the management of sensitive information. Its two controls are designed to ensure that organizations use cryptography properly and effectively to protect the confidentiality, integrity, and availability of data. | 6. Annex A.9 – Access control The aim of Annex A.9 is to ensure that employees can only view information that is relevant to their job.  It is divided into four sections, addressing the business requirements of access controls, user access management, user responsibilities and system and application access controls, respectively. 4. Annex A.11 – Physical and environmental security This annex addresses organization’s physical and environment security.  The objective of Annex A.11.1 is to prevent unauthorized physical access, damage or interference to organization’s premises or the sensitive data held therein.  Meanwhile, Annex A.11.2 deals specifically with equipment. It is designed to prevent the loss, damage, or theft of an organization’s information asset containers – whether that’s, for example, hardware, software or physical files. |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | END |  |  |