ISO 27001 Annex : A.14.2 Security in Development and Support Processes

ISO 27001 Annex : A.14.2 Security in Development and Support Processes It's objective is ensuring the creation and implementation of **information security** in the information system development process.

A.14.2.1 Secure Development Policy

Control- Regulations for software and system development should be laid down and applied to organizational developments.
Implementation Guidance – Secure development includes a safe infrastructure, architecture, software, and system to be developed. The following considerations should be taken into account in a stable technology policy:

1. Environmental development security;
2. security guidelines for the life cycle of software development:

- security in the methodology for software development;
- Secure guidelines on code for each language of programming used;

3. Design-phase protection requirements;
4. **Security control** points within the milestones of the project;
5. secure repositories;
6. Version control security;
7. Necessary security knowledge of application;
8. The ability of the developers to avoid, identify and fix **vulnerabilities**.

secure programming technology can be used for both software development and code replication situations where development requirements are not established or in line with existing best practices. The secure and, if applicable, mandatory coding criteria for use should be taken into account. Developers should be trained and their use should be verified for testing and code review.
The organization will be confident if development is outsourced that it complies with these principles of safe development.
Related Product : ISO 27001 Lead Auditor Training And Certification ISMS
Other information – Applications like office software, scripts, browsers, and databases can also be developed.
A well-known ISO 27001 Lead Auditor and ISO 27001 Lead Implementer certificate that mainly covers information security clauses and their implementation, i.e., controls which should be implemented by the organization to preserve the CIA triad, Confidentiality, Integrity, and Availability to maintain their critical, sensitive information in a secure manner. ***Infosavvy****, an institute in Mumbai conducts training and certification for multiple domains in Information Security which includes IRCA CQI ISO 27001:2013* ***Lead Auditor (LA)****,* ***ISO 27001 Lead Implementer (LI)*** *(TÜV SÜD Certification). Infosavvy will help you to understand and recognize the full scope of your organization's security checks to protect your organization's activities and information equipment (assets) from attacks, and also to illustrate the Controls for Protecting Application Software and their maintenance. We have trainers with extensive expertise and experience to ensure the efficient handling of the security of information. Consequently, the applicant will gain the necessary skills for the ISMS audit by using commonly agreed audit concepts, procedures and techniques.*
Read More : https://info-savvy.com/iso-27001-annex-a-14-2-security-in-development-and-support-processes/

This Blog Article is posted by

Infosavvy, 2nd Floor, Sai Niketan, Chandavalkar Road Opp. Gora Gandhi Hotel, Above Jumbo King, beside Speakwell Institute, Borivali West, Mumbai, Maharashtra 400092

Contact us – www.info-savvy.com