ISO 27001:2022 | ISO 27002:2022

ANNEX A CLAUSE 8.26 APPLICATION SECURITY REQUIREMENTS.

Control Type	Infosec Properties	Cybersecurity concepts	Operational capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application Security	#Protection #Defense

Control Statement

Information security requirements should be identified, specified and approved when developing or acquiring applications.

Requirement

Organizations may choose to develop bespoke applications internally organizations may choose COTS applications and customize them. In either case the security requirements should be identified and addressed prior the applications are rolled out to production. The requirements should be a part of entire acquisition and development cycles.

Implementation

This control combines and then expands two controls from ISO 27001:2013
A.14.1.2 – Securing Application services on Public Networks
A.14.1.3 – Protecting Application Services transactions

If an organization is using IT Applications for transactions (e.g. online Payments, ecommerce, Finance both B2B & B2C) and these applications are accessible over a public network e.g. Internet then controls should be put in place to ensure confidentiality and integrity of the transactional applications and prevent instances like unauthorized disclosure, alteration, duplication, incomplete transmission etc. This can be achieved using a Risk Assessment methodology. A Risk Assessment will determine the level of protection required. Some controls that are recommended are use of cryptographic controls like TLS that provide confidentiality via encryption, integrity via hashing and digital signatures for authenticity. Also additional methods like mandatory MFA during login and secondary authentication mechanism like an OTP for transaction may be required.
One standard that mandates this is PCIDSS that is to be used by all merchants that deal in online payments via payment cards (Visa/MasterCard). Both visa and MasterCard have implemented features like "Verified by Visa" and "MasterCard Secure code". Organizations may be subject to additional regulations from the governments for all transactional services.

ISO 27001:2022 | ISO 27002:2022

ANNEX A CLAUSE 8.26 APPLICATION SECURITY REQUIREMENTS.

Control Type	Infosec Properties	Cybersecurity concepts	Operational capabilities	Security Domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application Security	#Protection #Defense

Some requirements that can be considered and according needs controls are –

- **Classification Level of the Information**
- **Information contains PII or PHI**
- **Encryption Requirements – Does application need to be encrypted internally as well?**
- **Requirements as per legal and regulatory standards like HIPAA, GDPR etc.**
- **Logging and Monitoring Requirements**
- **Privacy Requirements**
- **Data Protection & Data Leakage Prevention**
- **Encryption Requirements (At Rest and In Transit)**
- **Protection against malware and other attacks like XSS & SQL Injection**
- **Input & Output Controls**
- **Storage Requirements- Data Localization and Data Retention.**

There can be multiple other controls that might be required. Detailed risk assessments and careful determination of controls are indispensable.

Applications that involve electronic ordering & payments (Commercial & Financial Applications) may require additional controls determined by local, provincial and federal laws around electronic payments and other regulations like PCIDSS.
One of the important controls is verification of the transactional information and payment information in addition to maintaining confidentiality, Integrity and Availability.