e main goals of an ISMS which are the CIA triad and the AAA concepts.

ISO 27001	OWASP Proactive Controls	OWASP Application Verification Standard	Control	Description
5.8 8.25 8.26	C1	1.1.5	Verify definition and security analysis of the application's high-level architecture and all connected remote services.	
5.8 8.25 8.26		1.1.4	Verify documentation and justification of all the application's trust boundaries, components, and significant data flows	
5.8 8.25 8.26		1.1.3	Verify that all user stories and features contain functional security constraints, such as "As a user, I should be able to view and edit my profile. I should not be able to view or edit anyone else's profile"	
5.8 8.25 8.26		1.1.2	Verify the use of threat modeling for every design change or sprint planning to identify threats, plan for countermeasures, facilitate appropriate risk responses, and guide security testing	
5.37		1.1.7	Verify availability of the secure coding checklist, security requirements, policy to all developers and testers.	
Confidentiality				
5.12 5.13		1.8.1	Verify that all sensitive data is identified and classified into protection levels and based on the Data Classification Policy.	
8.24	C6	2.4.1	Passwords SHALL be salted and hashed using an approved one-way password hashing function.	
8.5		2.5.2	Verify password hints or knowledge-based authentication (so called "secret questions") not present	
8.5 5.33	C6	2.5.3	Verify password credential recovery does not reveal the current password in any way	
8.24		2.9.1	Verify that cryptographic keys used are stored securely and protected against disclosure, such as using a Trusted Platform Module (TPM) or Hardware Security Module (HSM), or an OS service that can use this secure storage.	
5.33		3.1.1	Verify the application never reveals user identifiers ex. session tokens or users IDs, in URL parameters.	
8.24 5.34			Verify that regulated private data (PII), sensitive/Critical data, financial accounts is stored encrypted while at rest	
8.24	C8	9.1	Ensure all client messages are sent over encrypted networks, using TLS 1.2 or later.	
8.11 5.34			All sensitive data, including personally identifiable information (PII) and health information (PHI), must be masked in non-production environments to prevent unauthorized access during development and testing.	
8.33			Ensure that testing and validation processes are properly conducted on masked data to confirm that the masking does not interfere with the functionality and performance of applications	
Integrity				
8.28	C5	1.5.3	Verify that input validation is enforced on all user inputs in an apprioperiate way for each input type.	
8.28	C5	5.1.3	Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists).	
8.28	C3	5.3.4	Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries	
8.28		12.2.1	Verify that files obtained from untrusted sources are validated to be of expected type based on the file's content not only the extention and an allow-list.	
8.28	C4	5.3	Always encode output when rendering user-generated content.	
Availability				
		12.1.1	Verify that the application will not accept large files uploading.	
8.7		12.4.2	Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload and serving of known malicious content.	
5.29			The system must be designed with redundancy and failover mechanisms to ensure high availability, with regular testing and maintenance to minimize downtime and ensure business continuity in the event of a failure or attack.	
5.26			The system must follow the defined incident response plan	
			Regular load testing and stress testing must be conducted to ensure that the system can handle expected and unexpected traffic spikes without compromising availability.	
5.29 8.13			Backup systems must be implemented with a defined frequency and tested regularly to ensure data recovery can be performed quickly in the event of an outage.	
8.8		2.2.1	Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.	
Authentication				
8.5	C7	1.4.4	Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.	
8.5	C6		Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined)	
8.5	C6	2.1.2	Verify that passwords of at least 64 characters are permitted, and that passwords of more than 128 characters are denied	
8.5		2.1.6	Verify that password change functionality requires the user's current and new password.	
8.5		2.1.8	Verify that a password strength meter is provided to help users set a stronger password.	
8.5		2.3.1	Verify system generated Time-based OTP (TOTPs) SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time.	
8.5			Verify the application requires a secondary verification before allowing any sensitive transactions and critical functions, such as but not limited to, forgotten password.	
8.5			Verify forgotten password function use a secure recovery mechanism, i.e. time-based OTP	
8.5			Verify administrative portal use appropriate multi-factor authentication to prevent unauthorized use	
Authorization				

5.3			Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security)
5.15		4.1.1	Verify that the application enforces access control rules on a trusted service layer	
5.18	C7	4.1.3	Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization for the shortest time.	
Accountability				
8.15	C9	1.7.1	Verify that a common logging format and approach is used across the system.	
5.25 5.33	C9	1.7.2	Verify that logs are securely transmitted to a preferably separate system for analysis, detection, alerting, and escalation	
5.33	C9	7.1.1	Verify that the application does not log credentials	
5.33	C9	7.1.1	Session tokens should only be stored in logs in an irreversible way	

ISO 27001	OWASP Proactive Controls	OWASP Application Verification Standard	Control	Description
Session Management				
8.28	C6	3.2.1	Verify the application generates a new session token on user authentication.	
8.24	C6	3.2.4	Verify that session tokens are generated using approved cryptographic algorithms.	
8.28	C6	3.3.1	Verify that logout and expiration invalidate the session token	
8.28	C6	3.4	Verify that cookie-based session tokens have the 'Secure', 'HttpOnly', and 'SameSite: Lax' attributes set.	The cookie would only be sent over HTTPS, not accessible via JavaScript, and not sent with cross-site requests, providing a robust layer of security.
Errors and Exceptions				
	C10	4.1.5	Verify that access controls fail securely including when an exception occurs.	
	C10	6.2.1	Verify that all cryptographic modules fail securely, and errors are handled	
	C10	7.4.1	Verify that a generic message is shown when an unexpected or security sensitive error occurs	
Configuration Parameters Management				
8.9	C2	14.2.2	Verify that all unneeded features, documentation, sample applications and configurations are removed.	

ISO 27001	OWASP Proactive Controls	OWASP Application Verification Standard	Control	Description
Deployment Environment				
8.24		14.4.5	Verify that a Strict-Transport-Security header is included on all responses and for all subdomains	
8.31			production deployment environments must be configured according to security best practices, including the use of firewalls, intrusion detection systems, and secure network configurations to protect against unauthorized access and attacks.	
5.18 8.31			Access to production environments must be restricted to authorized personnel only, with role-based access controls enforced and regularly reviewed.	
8.8			All servers in the deployment environment must be regularly patched and updated to protect against known vulnerabilities, with a documented patch management process in place.	
Archiving				
5.34			Sensitive data must be archived securely using encryption and access controls to ensure that only authorized personnel can retrieve or restore archived data.	
8.1			Archived data must be retained for a specific duration defined by legal and regulatory requirements, after which it must be securely deleted or anonymized.	
8.15 8.16			Archiving mechanisms must include logging and monitoring to detect unauthorized access or anomalies during the data retrieval process.	
Anti-piracy				
5.32		10.3.1	Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed.	
5.32		10.3.2	Verify that the application employs integrity protections, such as code signing or subresource integrity	

ISO 27001	OWASP Proactive Controls	OWASP Application Verification Standard	Control	Description
Sequencing and Timing				
8.17			All time-sensitive operations must include mechanisms to ensure data integrity and consistency, such as timestamps and sequence numbers, to prevent replay attacks and ensure that actions are executed in the correct order.	
8.17			Systems must implement mechanisms to synchronize time across all components to prevent discrepancies that could lead to security vulnerabilities or operational issues.	
8.15			All critical operations must generate audit logs that include timestamps, user identification, and operation details to facilitate forensic analysis and compliance reporting.	
International				
			Application should support English and Arabic Languages	
Procurement				
5.19			Third-party vendors must provide evidence of their security posture, including security certifications (e.g., ISO 27001, SOC 2)	
5.2			Contracts with third-party providers must include security clauses that define responsibilities for data protection, incident response, and compliance with relevant regulations.	