epas

Enterprise Password Analytics Solution

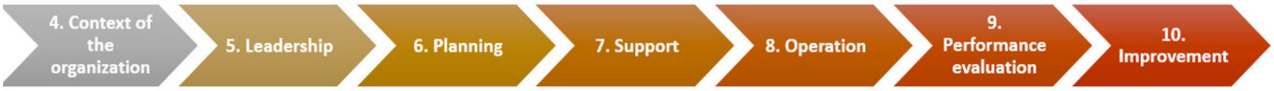
EPAS for Compliance: ISO/IEC 27001

Every organization that is implementing ISO/IEC 27001 compliance will have a password-based use. In this document, we are covering the requirements for passwords use that needs to be implemented.

The ISO/IEC 27001 security standard

ISO 27001 (officially known as ISO/IEC 27001:2013) is an international information security standard. This standard is used in an organization to implement, maintain, and to improve an information security management system (ISMS). Policies and procedures, including the legal, technical and physical controls involved in a company's IT risk management processes, are part of the ISMS.

ISO 27001 is split into 11 sections, plus Annex A covering the control objectives and controls. This standard represents a flexible framework that can be applied to different types of organizations of various sizes. For an organization to be compliant with ISO 27001, it has to address all requirements from sections 4 to 10, as presented in the figure below.


4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Scope of ISO/IEC 27001

- Indicates the specifications for initiating, enforcing, preserving and consistently improving an ISMS within an organisation.
- Incorporates specifications for the evaluation and management of data security risks customized to the requirements of the organisation.
- Allows the ISMS to "preserve the confidentiality, integrity and availability of information by applying a risk management process and to give confidence to interested parties that risks are adequately managed."[1]

"It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization."[1]

"The focal point of ISO 27001 is the requirement for planning, implementation, operation and continuous monitoring and improvement of a process-oriented ISMS."[2]

[1] ISO-IEC 27001:2013, Information technology: security techniques, information security management systems, requirements: ISO-IEC 27001:2013 (2013). Geneva.
[2] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

EPAS mapping over ISO 27001 controls

Implementing ISO 27001 supports organizations in blocking security risks, protecting sensitive data, and identifying the scope and bounds of their security programs. EPAS supports organizations into managing specific requirements. Following, EPAS features are mapped according to related ISO/IEC 27001:2013 control objectives and controls retrieved from Annex A.

A.5 Information security policies

A.5.1 Management direction for information security

A.5.1.1 Policies for information security: “A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.”[1]

✓ Password policies are part of the information security policies. EPAS Audit: provides a correct, factual basis upon which password policies will be defined. EPAS Enforcer: by enforcing the password policies, assurance is obtained by the fact that these policies are correctly known and applied by staff.

A.5.1.2 Review of the policies for information security: “The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.”[1]

✓ Ongoing analytics will determine whether or not password policies need to be adapted to address the evolution of threats. Revision history on password rules can be followed in the EPAS management console.

A.6 Organization of information security

A.6.2 Mobile devices and teleworking

A.6.2.1 Mobile device policy: “A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.”[1]

✓ Different classes of security can be defined in EPAS Audit and Enforcer, with defined sets of policies. Stricter rules can be defined for mobile/teleworking arrangements in order to increase security levels. Centrally managed mobile devices are supported.

A.6.2.2 Teleworking: “A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.”[1]

✓ Granular and location-specific classes can be defined in EPAS Audit and Enforcer, with defined sets of policies. Stricter rules can be defined for mobile/teleworking arrangements.

A.7 Human resources security

A.7.2 During employment

A.7.2.1 Management responsibilities: "Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization."[1]

✓ EPAS Audit provides a policy quality assurance mechanism, offering a central view on password quality versus password policies, across heterogeneous and distributed environments. Management has a clear set of metrics based on which to implement controls and processes are in place to quality assure passwords. The authentication-related security risks are no longer an unknown, but a measurable and actionable-upon fact. Potential liability for failing to assess the password security risks and remediate them are avoided.

A.7.2.2 Information security awareness, education and training: "All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function."[1]

✓ EPAS Audit supports organisations to directly address human-side risks by measuring awareness and training to users, based on password audit reports. History of password audit results allow for training effectiveness measurement and escalating information and training for riskier users.

✓ Independent from the audit feature, EPAS provides a separate interface for voluntary password quality evaluation that is normally employed by users to check passwords before using them; this interface is also used in awareness training. EPAS Enforcer provides direct feedback on password strength at password change, thus increasing awareness on security posture for all users.

A.7.2.3 Disciplinary process: "There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach."[1]

✓ In high-risk environments, enforcing strong passwords is a key element of access control. A strong deterrent against staff negligence is subjecting breaches of password policies to disciplinary process. In such delicate cases, EPAS Audit can provide needed evidence, without exposing key personal data that can be subject to privacy protection. EPAS can also measure how often a user has been informed about their poor password, yet neglected to address it.

A.8 Asset management

A.8.1 Responsability for assets

A.8.1.3 Acceptable use of assets: “Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.”[1]

✓ Password policies are a key element of acceptable use policies. With EPAS Audit, one can define and follow password policies tailored for different classes of assets and measure their implementation.

A.9 Access control

A.9.1 Business requirements of access control

A.9.1.1 Access control policy: “An access control policy shall be established, documented and reviewed based on business and information security requirements.”[1]

✓ Access rights management should leverage off digital identity attributes to determine the risk associated with a specific user's permissions. I.e. users with consistently weak passwords, which are detected by EPAS Audit, should have their access to sensitive assets reviewed.

A.9.2 User access management

A.9.2.1 User registration and deregistration: “A formal user registration and deregistration process shall be implemented to enable the assignment of access rights.”[1]

✓ User registration includes the creation of an account and allocation of an initial password that must be changed as soon as possible. EPAS Audit will determine if initial passwords are still in use, if they are shared amongst multiple users, and when such passwords have been changed. EPAS Audit data can be used to correlate registration/deregistration of accounts with the actual identities in the user repository.

A.9.2.2 User access provisioning: “A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.”[1]

✓ EPAS Audit will determine if initially provisioned passwords are still in use, if they are shared amongst multiple users, and when such passwords have been changed. EPAS Audit reports include detailed information about group and organizational unit membership, including nested groups belonging to a system.

A.9.2.3 Management of privileged access rights: “The allocation and use of privileged access rights shall be restricted and controlled.”[1]

✓ One-time solutions enable restrictions, while EPAS Audit allows defining stricter classes of password strength to be required for privileged accounts. Automatic notifications of violations and continuous metrics are used for provable strong authentication of privileged accounts.

✓ EPAS Enforcer is used to define stricter policies to be enforced for privileged accounts.

✓ EPAS components - Audit and Enforcer - are used either independently or complementing PAM (Privileged Access Management) solutions.

A.9.2.4 Management of secret authentication information of users: “The allocation of secret authentication information shall be controlled through a formal management process.”[1]

✓ EPAS analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS provides effective quality assurance for password-based authentication by using patented technology. EPAS provides all technical controls required by the formal management process described at point A.9.2.4.

A.9.2.5 Review of user access rights: “Asset owners shall review users’ access rights at regular intervals.”[1]

✓ EPAS Audit reports include detailed information about group and organizational unit membership, including nested groups. This enables fast identification of sensitive user rights, along with the password security metrics, for all accounts, including technical and accounts hard to identify.

A.9.2.6 Removal or adjustment of access rights: “The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.”[1]

✓ The EPAS Audit reports provide immediate insights on the security-related activities of accounts, such as last password change, last logon, lock status, and privilege related information. This data is instrumental in detecting and eliminating unused accounts that are still enabled and often have high privileges.

A.9.3 User responsibilities

A.9.3.1 Use of secret authentication information: “Users shall be required to follow the organization’s practices in the use of secret authentication information.”[1]

✓ EPAS Audit technology is used to both identify weak credentials that would expose secret information as well as shared credentials which would prevent accountability and would allow undetected data theft. EPAS Enforcer can prevent both weak access credentials as well as shared passwords.

A.9.4 System and application access control

A.9.4.2 Secure log-on procedures: “Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.”[1]

✓ EPAS analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS provides effective quality assurance for password-based authentication by using patented technology.

A.9.4.3 Password management system: “Password management systems shall be interactive and shall ensure quality passwords.”[1]

✓ EPAS analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS provides effective quality assurance for password-based authentication by using patented technology; point A.9.4.3 is entirely covered by EPAS without the need for additional measures or technologies.

A.10 Cryptography

A.10.1 Cryptographic controls

A.10.1.1 Policy on the use of cryptographic controls: “A policy on the use of cryptographic controls for protection of information shall be developed and implemented.”[1]

✓ EPAS Audit will detect and report clear-text passwords, passwords using reversible encryption, as well as passwords stored with weak/insecure hashing algorithms. Reporting metrics regarding all password algorithms used by an identity are embedded in the report content. This data can be instrumental in assisting implementing the controls specified by point A.10.1.1.

A.12 Operations security

A.12.4 Logging and monitoring

A.12.4.1 Event logging: “Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.”[1]

✓ EPAS Audit integrates into event logging systems by providing alerts when password quality falls below a certain threshold; it also triggers events when password audit reports are generated and available for examination.

✓ EPAS Enforcer provides granular and privacy compliant events whenever a password change occurs and whenever a password change fails due to password policy violations.

A.12.4.3 Operator logs: “System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.”[1]

✓ See A.12.4.1.

✓ See A.12.4.1.

A.12.7 Information systems audit considerations

A.12.7.1 Information systems audit controls: “Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.”[1]

✓ EPAS automatically retrieves account data for auditing, making use of encrypted channels, leveraging off vendor APIs/Connectors, and no agent/helper programs or similar entities are installed on target systems, hence no performance deterioration is observed, nor destructive impact is caused. Auditing can, therefore, be performed without any disruptions.

A.13 Communications security

A.13.1 Network security management

A.13.1.1 Network controls: “Networks shall be managed and controlled to protect information in systems and applications.”[1]

✓ EPAS Audit provides password quality metrics on centrally managed network devices using industry-standard authentication services.

A.13.1.2 Security of network services: “Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.”[1]

✓ EPAS Audit provides password quality metrics on centrally managed network devices using industry-standard authentication services.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

A.16.1.3 Reporting information security weaknesses: “Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.”[1]

✓ EPAS analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS provides effective quality assurance for password-based authentication by using patented technology. Automated alerts and messages can be triggered in order to be collected in incident management systems.

A.16.1.4 Assessment of and decision on information security events: “Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.”[1]

✓ Clear information on password weakness is readily available from EPAS Audit in the event of an incident, providing crucial information on event analysis and definition of response actions.

A.16.1.5 Response to information security incidents: “Information security incidents shall be responded to in accordance with the documented procedures.”[1]

✓ Through integration with SIEM or log management systems, EPAS password strength scoring can be used as an indicator of compromise. This can be used by analysts to prioritise events with a high probability of compromise (i.e. accounts with weak passwords)

A.16.1.6 Learning from information security incidents: “Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.”[1]

✓ EPAS Audit includes regularly updated password leaks obtained from known security incidents; this data is used by the password assessment process in order to determine if any of the accounts are using exposed credentials - such accounts are flagged immediately in order to start the remediation process. Previous reporting data can be leveraged to reduce the likelihood of misusing weak passwords.

✓ EPAS Enforcer is used to blacklist passwords that have already been exposed and are included in the leaked credentials database. Derivations are calculated on already compromised account credentials to enhance detection of weak credentials and reduce future risk.

A.16.1.7 Collection of evidence: “The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.”[1]

✓ Anti-fraud: Fine-grained audit trail of passwords and password history. Evidence can be provided that a user was regularly prompted to improve their password.

✓ Anti-fraud: Fraudulent insiders often claim that their accounts were hacked when their fraudulent behaviour has been detected. EPAS could demonstrate whether it was likely or not that their passwords could be hacked.

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

A.18.1.4 Privacy and protection of personally identifiable information: “Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.”[1]

✓ Personal identifiable information is protected by various means, but the access to such information is allowed or denied based on authentication and authorization. The first line of defense against enterprise attacks is represented by strong authentication, which in the majority of cases is based on a password. EPAS Audit provides all the relevant metrics to verify and prove that such data is protected by a password strong enough for the type of data it protects and that said password is unique and not leaked on any public medium.

A.18.1.5 Regulation of cryptographic control: “Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.”[1]

✓ EPAS Audit provides information on what password encryption/hashing algorithms are used in order to make sure that the cryptographic technology and level are in compliance with all relevant requirements. Clear text credentials and passwords stored with reversible encryption are immediately detected and reported.

A.18.2 Information security reviews

A.18.2.1 Independent review of information security: “The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.”[1]

✓ The authentication security review is a mandatory element of any IT security test. EPAS analyses password quality, by simulating a real attack, without ever exposing or storing the passwords and without risking the availability of the target system. EPAS Audit reports are designed to be objective and not changeable by organization, therefore, their content, results, will be independent from the user organization.

A.18.2.2 Compliance with security policies and standards: “Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.”[1]

✓ Passwords are the most used authentication method. EPAS Audit is used to prove that the currently used passwords' quality level corresponds to the strong authentication requirements of relevant security policies and standards.

A.18.2.3 Technical compliance review: “Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.”[1]

✓ Passwords are the most used authentication method. EPAS Audit is used to prove that the currently used passwords' quality level corresponds to the strong authentication requirements of relevant security policies and standards.

ISO/IEC 27001 controls supported by EPAS summary

ISO/IEC 27001 Controls	Description	EPAS Coverage
A.5.1.1	Policies for Information Security	✓
A.5.1.2	Review of the policies for information security	✓
A.6.2.1	Mobile device policy	✓
A.6.2.2	Teleworking	✓
A.7.2.1	Management responsibilities	✓
A.7.2.2	Information security awareness, education and training	✓
A.7.2.3	Disciplinary process	✓
A.8.1.3	Acceptable use of assets	✓
A.9.1.1	Access control policy	✓
A.9.2.1	User registration and de-registration	✓
A.9.2.2	User access provisioning	✓
A.9.2.3	Management of privileged access rights	✓
A.9.2.4	Management of secret authentication information of users	✓
A.9.2.5	Review of user access rights	✓
A.9.2.6	Removal or adjustment of access rights	✓
A.9.3.1	Use of secret authentication information	✓
A.9.4.2	Secure log-on procedures	✓
A.9.4.3	Password management system	✓
A.10.1.1	Policy on the use of cryptographic controls	✓
A.12.4.1	Event logging	✓
A.12.4.3	Administrator and operator logs	✓
A.12.7.1	Information systems audit controls	✓
A.13.1.1	Network controls	✓
A.13.1.2	Security of network services	✓

ISO/IEC 27001 Controls	Description	EPAS Coverage
A.16.1.3	Reporting information security weaknesses	✓
A.16.1.4	Assessment of and decision of information security events	✓
A.16.1.5	Response to information security incidents	✓
A.16.1.6	Learning from information security incidents	✓
A.16.1.7	Collection of evidence	✓
A.18.1.4	Privacy and protection of personally identifiable information	✓
A.18.1.5	Regulation of cryptographic controls	✓
A.18.2.1	Independent review of information security	✓
A.18.2.2	Compliance with security policies and standards	✓
A.18.2.3	Technical compliance review	✓

DETACK GmbH
Königsallee 43
71638 Ludwigsburg, Germany
Phone: +49 7141 69 62 65 0
Fax: +49 7141 69 62 65 5
info@detack.de
www.epas.de