epas

Enterprise Password Analytics Solution

EPAS for Compliance: Telecommunications Regulatory Authority - Information Assurance Regulation

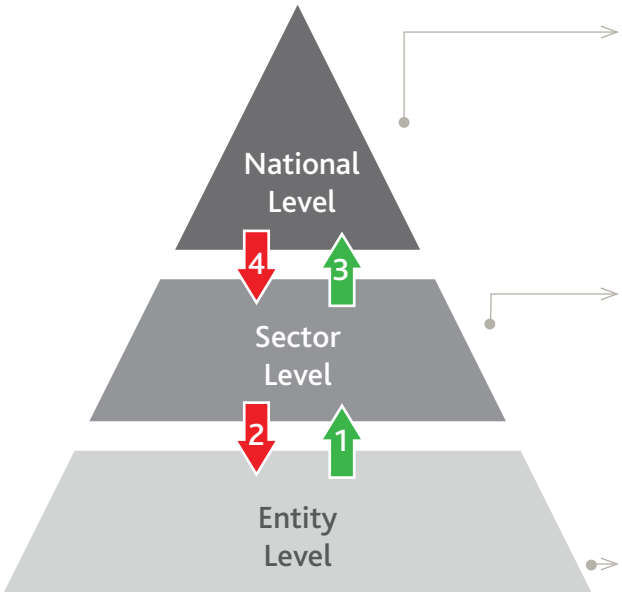
The TRA IAR security standard

A strategic priority for the UAE is managing cyber threats and assuring the implementation of a secure national communications and information infrastructure. Therefore, TRA implemented the UAE IA Regulation as a crucial component of the National Information Assurance Framework (NIAF) to specify prerequisites for enhancing the level of IA over all implementing organizations in the UAE. [1]

The UAE IA Standards grants technical and management data security controls to provide, develop, manage, and regularly update information assurance. [1]

EPAS mapping over TRA IAR requirements

TRA IA Regulation provides in-depth requirements for protection against cyber attacks, as well as indications of how to secure and maintain an IT infrastructure. The TRA IAR draws security relevant controls from existing standards (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27010, ISO/IEC 27032, NIST 800-53 R4, ADSICv1, ADSICv2, etc.) while enhancing subcontrols and providing in-depth information about example implementations. EPAS strongly assists organizations preventing breaches based on several TRA IAR recommendations, as detailed in the following pages. Following, the integrated relationships and interactions among individual sector entities implementing the TRA IAR are presented:



4 TRA consolidates and analyzes the information reported by sector regulators to from a national and sector view on the state of the Regulation implementation , as well as the risks , and shares relevant threat and risk information with sector regulators to increase effectiveness of the incident management and risk assessment programs.

3 Sector regulators consolidate and analyze information reported by entities to from a sector view of risks and the state of the UAE IA Regulation implementation, and escalate key findings to TRA and other Cyber Security parties.

2 Sector regulators share relevant security threat, risk and incident information with entities to increase effectiveness of the incident management and risk assessment programs

1 Entities report key information to sector regulators, in particular relating to;

- State of the UAE IA Regulation implementation.
- Risk assessment outcomes
- Cyber security threats, risks and incidents

1 Telecommunications Regulatory Authority - UNITED ARAB EMIRATES INFORMATION ASSURANCE REGULATION.
2 https://u.ae/-/media/guidelines/Guidelines-2020/UAE-IA-Regulation-v11-1.ashx

Control Number
M1.3.6
Control Name
Addressing Security When Dealing With Customers
Control Description
The entity shall address all identified security requirements before giving customers access to the entity's information or assets.
Sub-Control
The entity shall: 1) make sure that any customer accessing entity information and information systems are compliant with the entity's information security policy and security requirements 2) monitor any customer access and verify compliance to agreed access control policy
EPAS Coverage
EPAS Audit provides regular security checks for multiple enterprise systems which allow user authentication using passwords as an authentication factor. Customer access and compliance is directly provided through the use of the reporting functionality. For select system types, EPAS Audit allows granular investigation of access control policies (e.g. Active Directory, LDAP, IBM RACF). EPAS Enforcer allows the enterprise to enforce the use of strong passwords across systems, in order to ensure that customer access and authentication/authorization to entity information and information systems is done in a secure manner.

Control Number
M3.4.1
Control Name
Awareness Campaign
Control Description
The entity shall plan and conduct a security awareness campaign.
Sub-Control
The entity shall: 1) define the scope of the awareness campaign in terms of targets and content based on security risks relevant to users' activities 2) provide a timeline for deploying specific awareness campaigns to meet the program objectives 3) ensure that information security campaigns proceed according to the defined program timeline 4) identify alternative information security awareness campaigns if problems with the program timeline arise 5) ensure the updated information security awareness campaign satisfies all of the program objectives and needs identified
EPAS Coverage
EPAS provides adequate tooling for conducting awareness campaigns by use of the password quality evaluation page. This extends the coverage of awareness campaigns for both trainers and employees, by demonstrating, in real-time, the strength of passwords, as well as their reason for being rejected (e.g. passwords are present in known password leaks, are using common dictionary (or cultural) words or patterns). The EPAS administrator can change, modify and adapt the EPAS password policy and password requirements to the needs of the awareness campaigns and customize it to be in line with corporate policy.

Control Number
M4.4.3
Control Name
Removal of Access Rights
Control Description
The entity shall remove access rights of all stakeholders to information and information systems upon termination of their employment, contract or agreement, or adjusted upon change.
Sub-Control
The entity shall: 1) verify that the termination policy and procedure is followed for any termination or change of employment, contract or agreement with particular attention to revocation of credentials/access to any information facility
EPAS Coverage
EPAS Audit generates detailed password audit reports which also include critical information about the status of the termination process, whenever an employee, a contractor or a third party finish their employment. Multiple elements, part of the account information, can be analysed in case of termination: account expiration date, account disabled status, last login date, last password change date. The high number of supported systems for password storage (e.g. Windows, Active Directory, SAP, IBM RACF) provides additional coverage for all accounts of the terminated employee in the environment.

Control Number
T2.3.8
Control Name
Unattended User Equipment
Control Description
The entity shall ensure that unattended equipment has appropriate protection.
Sub-Control
The entity shall: 1) establish user responsibilities and procedures when leaving equipment unattended 2) configure equipment and systems to implement automatic protections when left unattended
EPAS Coverage
EPAS enhances the provided controls and sub-controls, by ensuring that the unattended equipment is sufficiently protected when the secure mechanisms implement password-based security.

Control Number
T5.2.1
Control Name
User Registration
Control Description
The entity shall implement a formal user registration and de-registration procedure.
Sub-Control
The entity shall: 1) establish and formalize procedures for the registration and de-registration of users 2) ensure that a separate account is created for each person requiring access, and prohibit sharing of same accounts across multiple users 3) immediately revoke access from users who have changed roles or jobs or left the entity following the established procedure 4) periodically check and revoke access related to temporary and inactive accounts

EPAS Coverage
EPAS Audit provides detailed information about the user registration and de-registration procedure, allowing the corporation to: assess the user account creation time, last logon, expiration date, while also ensuring passwords are not shared among users, as well as identifying shared passwords. This information is available on a periodical, enterprise-defined reporting period, and also enhanced with KPI analysis.

Control Number
T5.2.2
Control Name
Privilege Management
Control Description
The entity shall restrict and control the allocation and use of privileges.
Sub-Control
The entity shall: 1) maintain a record of all allocated privileges 2) never grant users with domain or local administrative privileges 3) ensure that administrator accounts are used only for system administration activities (e.g. no email or web surfing) 4) use two-factor authentication for all administrative access 5) ensure that all administrative access are logged and audited
EPAS Coverage
EPAS enhances the provided controls and sub-controls, by ensuring that the unattended equipment is sufficiently protected when the secure mechanisms implement password-based security. EPAS Enforcer implements granular password policies tailored for the privilege level of the user. Therefore, it is possible to enforce stronger password policy controls for users, based on their privilege level. All password policy checks are also logged for eventual audit validation.

Control Number
T5.2.3
Control Name
User Security Credentials Management
Control Description
The entity shall control the allocation of user security credentials.
Sub-Control
The entity shall: 1) establish a user security credential management policy for users and administrators that is appropriate to the purpose of the entity 2) ensure that the policy includes a secure process to provide users with security credentials; policy should also include credential revocation procedure and credential re-allocation. 3) in case of use of security credentials (i.e. passwords) change default security credentials of all systems and applications 4) in case of credentials, always store them in a well-hashed (including “salting”) or encrypted format 5) for accessing critical resources/assets, implement credential systems based on multi-factor authentication

EPAS Coverage
EPAS Audit allows the entity to control allocation of user security credentials, through the use of regular reporting features, as well as reuse and aggregate reports. With EPAS Audit, it is possible to verify that users are not using leaked passwords, or weak passwords based on common dictionary words, to verify that the account revocations procedures have been successful, to check that default passwords are not present, to check and report on the hashing algorithm of passwords. EPAS Enforcer prevents the usage of weak passwords and is directly implemented in the core credential allocation process. Therefore, accounts are no longer permitted to use weak, leaked, default or cryptographically insecure passwords.

Control Number
T5.2.4
Control Name
Review of User Access Rights
Control Description
The entity shall review users' access rights.
Sub-Control
The entity shall: 1) maintain access right records for all assets, and identify any granted special access 2) establish a access right review procedure to ensure access rights are reviewed periodically or on any changes in users' status 3) periodically check the granted special access to ensure their validity
EPAS Coverage
EPAS Audit allows, through the use of reports, monitoring particular systems for allocated privileges, on user accounts. The standard reporting functionality includes group membership, group information, for all the audited users, which is directly mapped to roles. Combined with the historical analysis and the presence of multiple reports in the history, it provides both access right records for assets as well as essential tools for the access right review procedure.

Control Number
T5.3.1
Control Name
Use of Security Credentials
Control Description
The entity shall require users to use security credentials in line with the entity's security practices.
Sub-Control
The entity shall: 1) develop a good practice for use of security credentials 2) share and educate users on the developed good practices through awareness and training sessions (refer to M3.2.1)
EPAS Coverage
EPAS Audit implements continuous monitoring of security credentials, and is directly involved in the development of good practice for use of the aforementioned credentials. Notable functionality which enhances the use of security credentials are: the public password checking and policy verification page (used in developing good practices when choosing passwords), the password policy verification during audits, as well as statistical analysis of weak passwords (password length, character frequency analysis and structural entropy).

Control Number
T5.4.7
Control Name
Wireless Access
Control Description
The entity shall ensure wireless access is secured.
Sub-Control
The entity shall: 1) establish usage restrictions, configuration requirements, and implementation guidance for wireless access 2) authorize wireless access to the information system prior to allowing such connections
EPAS Coverage
EPAS Audit allows regular auditing of Wireless (802.11x) communications which use passwords as an authentication factor. Moreover, for RADIUS based Wireless communication, it is also possible to generate reports for the authentication sources.

Control Number
T5.5.1
Control Name
Secure Log-On Procedures
Control Description
The entity shall control access to systems and applications using a secure log-on and log-off procedure.
Sub-Control
The entity shall: 1) identify the systems, applications and services that require user authentication 2) classify the identified systems, application and services based on the level of protection needed 3) establish the appropriate log-on and log-off procedures to minimize the opportunity for unauthorized access 4) set a maximum session time for logged on users for sensitive systems and applications 5) terminate inactive sessions after a predefined period of inactivity
EPAS Coverage
EPAS Audit supports auditing of most enterprise operating systems which support user authentication, enabling full coverage for technical accounts (applications) or services which require log on/off procedures; passwords are regularly audited and weak or default credentials are reported to the EPAS administrator. Subsequent classification of technical accounts, including mapping to relevant controls (password policies, password strength, access right management) is possible.

Control Number
T5.5.2
Control Name
User Identification and Authentication
Control Description
The entity shall create a unique identifier (user ID) for each user and implement a suitable authentication technique.

Sub-Control
The entity shall: 1) provide a unique identifier to each user 2) enable authentication techniques that are suitable to entity 3) ensure all restricted activity are logged with the associated authenticated users
EPAS Coverage
EPAS Audit permits auditing user credentials, which are used in the user identification and authentication process. Errors are generated whenever entities have duplicate identifiers. Report information contains the algorithm used for the authentication, allowing the verification of authentication techniques that are suitable to the entity.

Control Number
T5.5.3
Control Name
User Credentials Management System
Control Description
The entity shall implement a system for managing user credentials (i.e. passwords).
Sub-Control
The entity shall: 1) automate the user credential change procedure ensuring the authenticity of the associate user identity 2) validate that the changed credentials have sufficient strength for their intended use to ensure quality secret authentication 3) set a maximum lifetime and reuse conditions
EPAS Coverage
EPAS Enforcer controls the user credential change procedure for all accounts/users using passwords as an authentication mechanism. Validation that the used credentials are secure (password strength for their intended use) is a vital component of the Enforcer mechanism, and can be applied granularly to user groups, system groups or other structured user repositories.

Control Number
T5.7.1
Control Name
Access Control for Mobile Devices
Control Description
The entity shall adopt the appropriate security measures to protect against the risks of using portable and mobile devices.
Sub-Control
The entity shall: 1) establish security measures for usage restrictions, configuration/connection requirements, and implementation guidance for entity-controlled mobile devices in line with the access control policy (See T5.1.1) 2) authorize connection of mobile devices to organizational information systems in accordance with the established security measures
EPAS Coverage
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 (A/D, LDAP, etc.) are supported.

Control Number
T5.7.2
Control Name
Teleworking
Control Description
The entity shall implement security measures to protect information accessed, processed or stored on teleworking sites.
Sub-Control
The entity shall: 1) establish security measures for using teleworking in line with the access control policy 2) authorize the usage of teleworking in accordance with the established security measures
EPAS Coverage
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.

Control Number
T7.4.1
Control Name
POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS
Control Description
The entity shall establish a policy on the use of cryptographic controls
Sub-Control
The entity shall: 1) develop and document a policy for the use of cryptographic controls in line with the criticality of the information to be protected 2) ensure the policy takes into account the sector or national level restrictions including TRA's relevant issuances and guidance in this regard 3) share the policy with relevant users 4) review and update the policy at planned intervals or if significant changes occur
EPAS Coverage
EPAS will detect and report clear-text passwords, passwords using reversible encryption, as well as passwords stored with weak / insecure hashing algorithms.

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