WHITEPAPER

Mapping BeyondTrust Capabilities to the DESC - ISR v2.0

BeyondTrust

Table of Contents

Overview

This guide has been prepared so that IT and security administrators can quickly understand how BeyondTrust Privileged Access Management (PAM) solutions map into requirements set forth in the Dubai Electronic Security Center (DESC) - Information Security Regulation (ISR) v2.0.

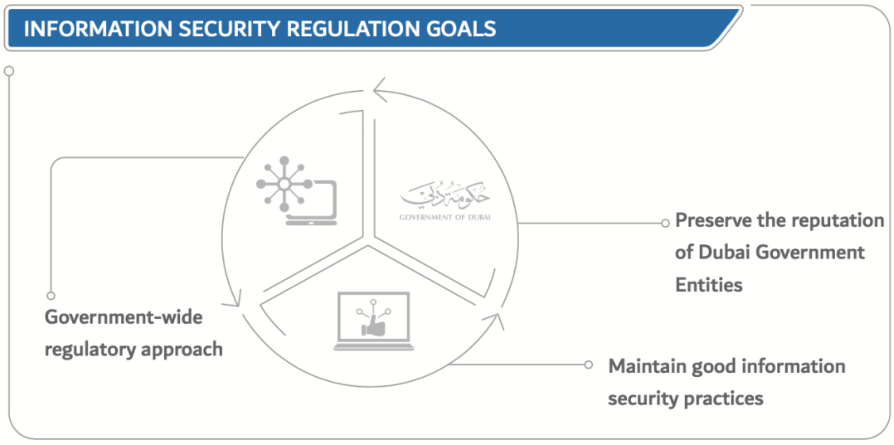
The Dubai Government Information Security Regulation provides key practices in information security to be adopted by all Dubai Government Entities (DGEs). It is designed to encourage the employees to adopt information security best practices and ensure the deployment of effective techniques to respond to information security incidents. In addition, the objective of this regulation is to establish an information security culture in all Dubai Government Entities. This culture will encourage Dubai Government Entities to integrate information security within their existing and future strategies.

Purpose

The purpose of the Information Security Regulation is to provide all Dubai Government Entities with the standards to ensure continuity of critical business processes and minimize information security related risks and damages by preventing and/or minimizing information security incidents. It intends to ensure appropriate level of Confidentiality, Integrity and Availability for information handled within Dubai Government Entities.

The goals of the Information Security Regulation are as follows:

A. To establish a Government-wide regulatory approach to information security.
B. To prescribe high-level mechanisms that help identify and prevent information security compromises in order to preserve the reputation of Dubai Government Entities.
C. To identify the responsibilities required to maintain good information security practices.

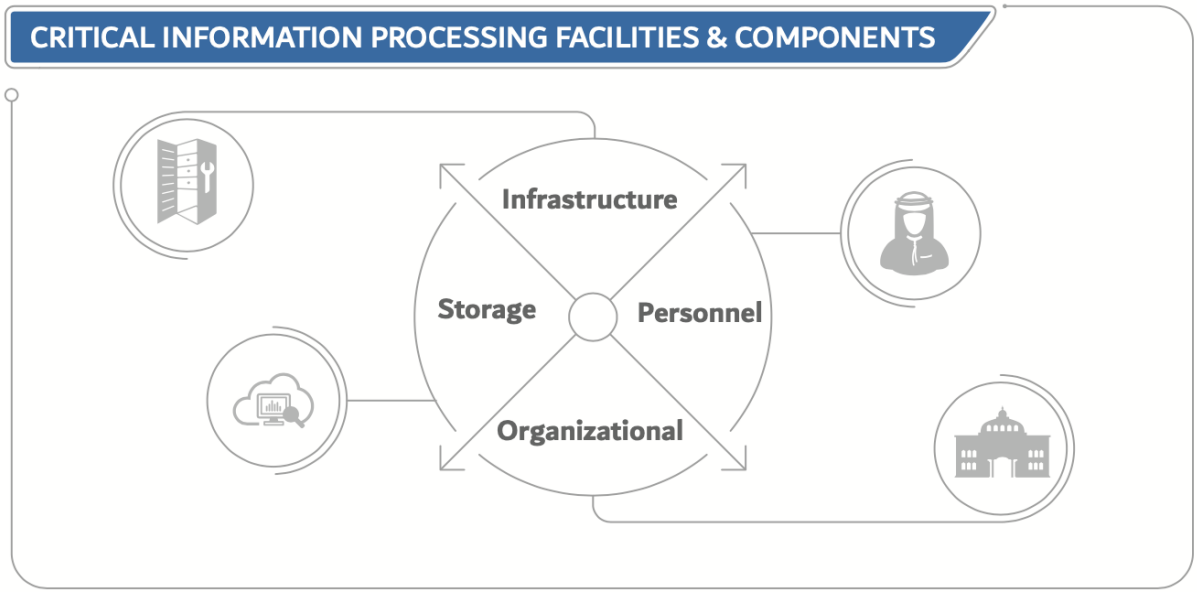


Source: Information Security Regulation, Version 2.0, Ref number 1a/2017, Dubai Electronic Security Center

Scope

The Information Security Regulation presents the minimum requirements for information security controls and is applicable to all Dubai Government Entities, including but not limited to employees, consultants, contractors and visitors who are not government employees but are engaged with it through various means.

Furthermore, the regulation applies to any government information regardless of its type and medium (e.g. Printed, Electronic and Non-Electronic Verbal, Written, etc.). Therefore, Dubai Government Entities are expected to implement this regulation in all the divisions/departments within an entity and not to limit the implementation to Information Technology (IT) divisions/departments only.



Source: Information Security Regulation, Version 2.0, Ref number 1a/2017, Dubai Electronic Security Center

The scope of the information security management program must consider all business processes and critical information processing facilities and components, including:

A. Storage (electronics storage device; logical and physical, paper documents, etc.)
B. Infrastructure (hardware, applications, networks, etc.)
C. Organizational (processes, policies, etc.)
D. Personnel (administrators, employees, visitors, etc.)

Information Security Regulation structure

The Information Security Regulation is broken down into thirteen domains. Each domain takes into consideration one or more major classes of information security: Governance, Operation, and Assurance:

- The Governance domains set high-level requirements for structuring and managing information security.
- The Operation domains are technical and/or non-technical controls an entity may use depending on the results of their risk assessment study.
- The Assurance domains act as the quality assurance for the entity, ensuring that the implemented solution is working as intended.

TABLE 1. INFORMATION SECURITY REGULATION DOMAINS AND CLASSES

DOMAINS	CLASSES		
	GOVERNANCE	OPERATION	ASSURANCE
Domain 1 – Information Security Management and Governance	✓		
Domain 2 – Information and Information Asset Management	✓	✓	
Domain 3 – Information Security Risk Management	✓	✓	
Domain 4 – IIncident and Problem Management		✓	
Domain 5 – Access Control		✓	
Domain 6 – Operations, Systems and Communication Management		✓	
Domain 7 – Business Continuity Planning	✓	✓	
Domain 8 – Information Systems Acquisition, Development and Management		✓	
Domain 9 – Environmental and Physical Security		✓	
Domain 10 – Roles and Responsibilities of Human Resources	✓	✓	
Domain 11 – Compliance and Audit	✓		✓
Domain 12 – Information Security Assurance and Performance Assessment	✓		✓
Domain 13 – Cloud Security	✓		✓

Source: Information Security Regulation, Version 2.0, Ref number 1a/2017, Dubai Electronic Security Center

The Information Security Regulation has been structured as follows:

A. Domains: Reflect a key process within information security
B. Objective: Reflects what is to be achieved from the domain
C. Controls: Reflect what is to be applied to achieve the objective
D. Sub Controls: Reflect subordinate detailed controls to the main control

How BeyondTrust Solutions Can Help

BeyondTrust capabilities mitigate 13 primary and secondary controls across 4 of the 13 main domains within the Dubai Electronic Security Center (DESC) - Information Security Regulation (ISR) v2.0.

This white paper explains how to map BeyondTrust solutions to the **DESC ISR v2.0** to maintain security and more easily demonstrate and maintain compliance. BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges.

Each **DESC ISR v2.0** policy requirement is outlined in the following sections and is mapped to these BeyondTrust solutions:

- (PPM) Privilege Password Management - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.

- (SRA) Secure Remote Access - Apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.

- (EPM) Endpoint Privilege Management - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

- (DSS) DevOps Secrets Safe - Secure and automate the storage and access of secrets used by applications, tools, and other processes across your development operations environments.

The table on the following page highlight the primary applicable **DESC ISR v2.0** requirements that are addressed by capabilities within BeyondTrust solutions. This is not an exhaustive list but includes the most relevant features for supporting the **DESC ISR v2.0** framework.

Ref Page #	Domain Name	Objective	Main Control	Control Description	Sub Control	Control Description	BeyondTrust Products			
							PPM	SRA	EPM	DSS
30	Information and Information Assets Management	To identify and classify the information assets, and define the proper storage and handling & secure disposal measures in order to protect the entity from legal liabilities, losses, attacks, etc.	Information Assets Management	2.1.2 Identifies, documents, and maintains a register of all critical information assets for the entire entity, including the information and data assets and the related information processing facilities and components, such as software assets, people assets, physical assets, etc. and consider other details such as information classification, physical location, license details, business value, and any other necessary information that may be required to avoid risks and recover from disasters.			●			
			Information Assets Ownership/Custodianship	2.2.3 Assigns the information assets owner the responsibility of defining the proper access control to the information and ensuring periodic review of access in accordance with assigned classification level and the entity's access control policy.			●			
42	Incident and Problem Management	To outline a proper process for the identification and effective handling of information security incidents in order to minimize the adverse impact on the business of the entity.	Evidence Gathering	4.3.1 Implement a process to gather and retain evidences related to any information security incidents.			●	●	●	
46	Access Control	To secure and protect the logical and physical access to entity's information, information processing facilities, and resources.	Logical Access Control		Users Access Control	5.2.1.1 Defines and implements a process for users registration, de- registration, and users access privileges modification, disabling or removal, etc. 5.2.1.2 Provides each user with a unique identifier (user ID) for their individual business use only. 5.2.1.3 Implements a unified users ID standard across the entity. 5.2.1.4 Implements a proper authentication technique for the validation of claimed identities of users regarding access being onsite and remote. 5.2.1.5 Develops, distributes and maintains appropriate authentication policy (ies) (e.g. a password management policy that clearly addresses the password allocation process, users' responsibilities on passwords use and the recommended password structure, etc.). 5.2.1.6 Identifies the categories of users requiring regular and special privileges by ensuring the availability of the following: * A valid and approved access authorization. * Intended system usage. * Other attributes as required by the entity or associated missions/ business functions. * Utilization of access accounts with special privileges must be restricted for their intended purpose. 5.2.1.7 Maintains records of all users' access privileges, and monitors them on a continuous basis. 5.2.1.8 Limits the number of special/high privileged user IDs to those individuals who absolutely must have such privileges for authorized business purposes. 5.2.1.9 Implements proper security and independent monitoring controls over the usage of special or high privileged IDs. 5.2.1.10 Implements proper process for guest and temporary user IDs request and employs automated user IDs termination. 5.2.1.11 Allocates access privileges on a restricted basis while employing least privilege concept and separation of duties. 5.2.1.12 Employs a process for review and re-authorization of user access rights on a periodic basis, as defined by the entity.	●	●	●	●
48					Network Access Control	5.2.2.1 Develops, distributes and maintains a policy for network access control, which covers details about accessible networks and networks services, authorization process for granting network access, etc. 5.2.2.2 Defines a process for authorizing, activating and terminating any network connections in the entity. 5.2.2.3 Implements a proper network access control tool/method for network equipment/devices connectivity detection, identification and authentication. 5.2.2.4 Implements proper authentication tool for remote access connections.	●	●		
50					Operating System Access Control	5.2.3.2 Assigns each user with a unique user ID and apply the proper authentication method for identity verification. 5.2.3.3 Limits the use of generic user IDs to only exceptional and business justified circumstances, and implements the proper accountability technique for such use. 5.2.3.5 Manages and controls the use of utility programs. 5.2.3.8 Restricts connection times for critical information systems and applications. 5.2.3.9 Records and continuously reviews logs of administrators system IDs.	●	●	●	
50					Applications Access Control	5.2.4.1 Provides access to applications based on job responsibilities and business justifications, in alignment with the entity access control policy/ procedure. 5.2.4.2 Implements proper physical or logical isolation controls for highly critical information systems and application environments.	●	●	●	
52					Remote Access Security	5.2.5.1 Develops, distributes and maintains a policy addressing remote access to the entity's resources. 5.2.5.2 Enforces formal authorization prior to remote access connections. 5.2.5.4 Provides remote access users with access to the services, which the users are specifically authorized to use. 5.2.5.5 Monitors and periodically reviews the remote access connections logs.	●	●	●	
56			Access Control Audit and Review	5.6.1 Implements audit trails in information processing systems, as necessary. 5.6.2 Logs, maintains and periodically reviews logical and physical access control lists.			●	●		
60	Operation, Systems and Communication Management	To set controls for mitigating the risks associated with the daily operations of information processing systems, applications, network and communication tools being used internally and/or with external party.	Operations Management		Segregation of Duties	6.1.4.1 Segregates duties and responsibilities as necessary through distributing the tasks for a specific business process / area among multiple users, in a manner to reduce errors, fraud and unauthorized modification or misuse of the entity's assets.	●	●	●	●
62					Separation of Operational Facilities	6.1.5.1 Segregates where necessary development, testing and production processing facilities to mitigate the risk impacting the production systems from unauthorized intentional or unintentional access or change.	●	●	●	
70			Monitoring and Logs Management	6.9.2 Sets adequate monitoring requirements for all information systems/ applications based on criticality of the systems. 6.9.3 Logs system administrators and operators activities and ensures reviewing them periodically, by an independent unit.			●	●	●	
81	Information Systems Acquisition, Development and Management	To protect information from unauthorized modification or misuse through the integration of information security into the Systems Acquisition/Development Life Cycle.	Cryptography Controls	8.8.1 Develops, distributes and maintains a policy on the use of cryptography and key management wherever applicable (e.g. during development and maintenance of information systems/applications etc.). 8.8.2 Implements proper cryptography and key management mechanisms as required by the entity. 8.8.3 Implements proper protection and security controls on all cryptographic keys used by the entity.			●			●

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.