BeyondTrust

WHITEPAPER

BEYONTRUST AND THE UAE INFORMATION ASSURANCE STANDARD

Mapping BeyondTrust Capabilities to the UAE Information Assurance Standard

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 UAE Information Assurance Standard (IAS) as defined by the National Electronic Security Authority (NESA).

What is the UAE Information Assurance Standard?

The adoption of Information Technology (IT) and electronic communication have greatly improved the efficiency and productivity of businesses and governments within the UAE and facilitated collaboration of individuals within the nation and across the globe. Undoubtedly, IT and electronic communication have and will continue to play a pivotal role in the economic development of the UAE and the daily life of its citizens.

Therefore, the UAE stands committed to the further development of its national IT and electronic communication infrastructure, as well as its cyberspace, to support economic development and provide an environment where the interests of its governments, businesses, and citizens can thrive.

The benefits of this technology adoption, however, come with a rapidly evolving set of cyber threats. These threats stem from a wide range of sources – including hacktivists, issue-motivated groups, and organized cybercrime syndicates – and represent national security concerns that can potentially disrupt critical national services and compromise critical information assets.

Mitigating cyber threats and ensuring the development of a secure national information and communications infrastructure, and cyberspace, is a strategic priority for the UAE. To this end, NESA developed the UAE IA Standards as a critical element of the National Information Assurance Framework (NIAF) to provide requirements for elevating the level of IA across all implementing entities in the UAE.

The development of the UAE IA Standards is based on regional and global best practices including:

- ISO/IEC 27001:2005 “Information technology - Security techniques – Information security management systems - Requirements”
- ISO/IEC 27002:2005 “Information technology - Security techniques - Code of practice for Information security management”
- ISO/IEC 27005:2005 “Information technology - Security techniques -Information security risk management”
- ISO/IEC 27010:2012 “Information technology - Security techniques – Information
- Security management for inter-sector and inter-organizational communications”
- ISO/IEC 27032:2012 “Information technology - Security techniques – Guidelines for cybersecurity”
- NIST 800-53 Revision 4 “Security and Privacy Controls for Federal Information Systems and Organizations”
- Abu Dhabi Information Security Standards Version 1 and Version 2, developed by Abu Dhabi Systems and Information Centre (ADSIC)
- SANS 20 Critical Security Controls for Effective Cyber Defense Version 4.1

Additionally, the development was guided by key principles including:

- Applicability of the common IA requirements across industries , and applicability of the sector-specific IA requirements across entities within each CIIP sector
- Support for the development of the entity, sector, and national-level views of cyber security, to address potential IA risks that emerge from the interconnectivity of entities and sectors

- Support the performance management and the evolution of the controls in these standards based on measuring and sharing effective performance indicators, as well as contributions from key stakeholders to support the ongoing development and refinement of these Standards

Who Needs To Implement The UAE Information Assurance Standard?

Compliance with these Standards will raise the level of information assurance within the United Arab Emirates and help the United Arab Emirates progress towards a more resilient national information and communication infrastructure, and cyberspace.

All UAE government entities and other entities identified as **critical**[1] by NESA are obligated to implement these Standards. However, NESA highly recommends all entities in the UAE to adopt these Standards on a voluntary basis, as applicable, in order to participate in raising the nation minimum-security levels.

[1] The process for NESA to designate an entity as "critical" is outlined in the UAE Critical Information Infrastructure Protection (CIIP) Policy produced by NESA.

Prioritization Of Controls

The concept of Prioritization relates to grouping the UAE IA Standards security controls in order of importance for realizing a minimum level of information assurance protection, and for enabling a phased and incremental implementation of these Standards.

The prioritization approach of the UAE IA Standards is based on the relative impact of security controls in helping implementing entities to:

- Mitigate common threats
- Build foundational IA capabilities

Based on these criteria, the security controls are grouped into four priority levels – P1, P2, P3, and P4 in this order of importance – and the outcome of the prioritization is included in Annex 2.

While all the applicable security controls across the four priority levels are mandatory for critical entities implementing these Standards, they are required to begin implementing these Standards with P1 security controls given their highest relative impact in protecting against critical threats and building foundational information assurance capabilities.

Critical entities implementing these Standards may alter (promote or demote) the suggested priority of controls based on the outcomes of their risk assessment, with the exception of top priority controls (P1), which if applicable, may be augmented but never reduced.

How BeyondTrust Solutions Can Help

BeyondTrust capabilities address 25 Technical and Management controls in the UAE information assurance standard, of which 14 are P1 requirements, 8 are P2 requirements, 1 P3 requirement and 2 P4 requirements.

Each UAE IAS requirement is outlined in the next section and are mapped to these BeyondTrust solutions:

- **Privilege Password Management (PPM)** - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities
- **Secure Remote Access (SRA)** - Apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks
- **End Point Privilege Management (EPM)** - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity
- **DevOps Secrets Safe (DSS)** - Secure and automate the storage and access of secrets used by applications, tools, and other processes across your development operations environments

This is not an exhaustive list but includes the most relevant features for supporting NESA IAS compliance.

Mapping BeyondTrust Solutions to the UAE Information Assurance Standard

Strategy and Planning

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
M1.3.5	Identification Of Risks Related To External Parties	P1	Based on risk assessment	Where there is a need to allow an external party access to the information systems or information of an entity, a risk assessment should be carried out to identify any requirements for specific controls. The identification of risks related to external party access should take into account the following issues: A. The information systems an external party is required to access B. The type of access the external party will have to the information and information systems, e.g. 1- Physical access, e.g. to offices, computer rooms, filing cabinets 2- Logical access, e.g. to an entity's databases, information systems 3- Network connectivity between the entity's and the external party's network(s), e.g. permanent connection, remote access 4- Whether the access is taking place on-site or off-site C. The value and sensitivity of the information involved, and its criticality for business operations D. The controls necessary to protect information that is not intended to be accessible by external parties	●	●	●	
M1.3.6	Identification Of Risks Related To External Parties	P1	Based on risk assessment	Where there is a need to allow an external party access to the information systems or information of an entity, a risk assessment should be carried out to identify any requirements or specific controls. The identification of risks related to external party access should take into account the following issues: A. The information systems an external party is required to access	●	●	●	

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				B. The type of access the external party will have to the information and information systems, e.g. 1- Physical access, e.g. to offices, computer rooms, filing cabinets 2- Logical access, e.g. to an entity's databases, information systems 3- Network connectivity between the entity's and the external party's network(s), e.g. permanent connection, remote access 4- Whether the access is taking place on-site or off-site C. The value and sensitivity of the information involved, and its criticality for business operations D. The controls necessary to protect information that is not intended to be accessible by external parties				

Human Resources Security

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
M4.3	During Employment		Always applicable	Reg. Abuse of system access/privileges	●	●		
M4.3.2	Disciplinary Process	P2	Always applicable	In serious cases of misconduct, the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.	●	●		

Asset Management

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T1.2.1	Inventory of Assets	P2	Based on risk assessment	The entity shall maintain an inventory list of all its information assets. Here is a list of inventory assets that might be considered including, but not limited to: HARDWARE - SERVER • Laptops, workstations, storage, security devices (firewall, IDS / IPS, anti-spam, etc.) NETWORK • Routers, gateways, switches, Wireless Access Points, network segments (e.g. cabling and equipment between two computers), Others (SAT, Laser)	●	●		

Operations Management

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T3.2	Operational Procedures And Responsibilities		Always applicable	Abuse of system access/privileges	●	●	●	
T3.2.3	Change Management	P4		Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information should be retained.	●	●	●	
T3.2.4	Segregation Of Duties	P2	Based on risk assessment	Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls. Small entities may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.	●	●	●	
T3.4.1	Controls Against Malware	P1	Based on risk assessment	The entity shall protect its information assets from malware.			●	
T3.6	Monitoring			To detect, prevent and correct the use of systems and information based on audit logs of events that could impact the security of an entity. Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of	●	●	●	

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				servers, should be configured to create access control logs when user attempts to access resources without the appropriate privileges.				
T3.6.2	Audit Logging	P2	Based on risk assessment	The entity shall produce and keep audit logs recording user activities, exceptions, and information security events. Entities should log local and remote access (including failed attempts) to and from all hardware devices, operating systems and installed applications, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Audit logs should include, when relevant: A. User IDs B. Dates, times, and details of key events, e.g. log-on and log-off C. Terminal identity or location if possible D. Records of successful and rejected system access attempts E. Records of successful and rejected data and other resource access attempts F. Changes to system configuration G. Use of privileges H. Use of system utilities and applications I. Files accessed and the kind of access J. Network addresses and protocols K. Alarms raised by the access control system L. Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems	●	●		
T3.6.3	Monitoring System Use	P1	Based On Risk Assessment	The level of monitoring required for individual systems should be determined by a risk assessment. An entity should comply with all relevant legal requirements applicable to its monitoring activities. Areas that should be considered include: A. Authorized access, including detail such as: 1- The user ID 2- The date and time of key events	●	●	●	

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				3- The types of events 4- The files accessed 5- The program/utilities used B. All privileged operations, such as 1- Use of privileged accounts, e.g. supervisor, root, administrator 2- System start-up and stop 3- I/O device attachment/detachment 4- Deleting, creating and granting privileges activities C. Unauthorized access attempts, such as: 1- Failed or rejected user actions 2- Failed or rejected actions involving data and other resources 3- Access policy violations and notifications for network gateways and firewalls 4- Alerts from proprietary intrusion detection systems D. System alerts or failures, such as: 1- Console alerts or messages 2- System log exceptions 3- Network management alarms 4- Alarms raised by the access control system E. Database activities, such as: 1- Use of privileged accounts 2- Backup / restore 3- Failed or rejected user actions F. Changes to, or attempts to change, system security settings and controls. Please refer to detailed note.				
T3.6.5	Monitoring System Use	P2	Based On Risk Assessment	The entity shall log system administrator and system operator activities.	●	●	●	

Communications

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T4.4	Information Sharing Protection			Misappropriation of private knowledge • Abuse of system access/privileges	●	●	●	
T4.5	Network Security Management			• Abuse of system access/privileges	●	●		

Access Control

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T5.1	Access Control Policy			• Unsuitable access control policy	●	●	●	
T5.1.1	Access Control Policy	P2	Based On Risk Assessment	The policy should take account of the PRIVILEGE ACCESS ROLES (among others). Please refer to the control for more information.	●	●	●	
T5.2	User Access Management			To ensure authorized user access and to prevent unauthorized access to information systems. One way of automation is to use identity management systems to manage accounts, their authentication, authorization, roles, and privileges. RELEVANT THREATS AND VULNERABILITIES • Use of stolen login credentials • Brute force and dictionary attacks • Authentication bypass	●	●	●	
T5.2.1	User Registration	P1	Based On Risk Assessment	A. Using unique user IDs to enable users to be linked to and held responsible for their actions; the use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented	●	●		

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				B. Verifying that the user has authorization from the owner of the information system or service for the use of the information system or service; separate approval for access rights from management may also be appropriate				
T5.2.2	Privilege Management	P1	Based On Risk Assessment	The entity shall restrict and control the allocation and use of privileges. 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 Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process in accordance with the relevant access control policy. The following steps should be considered: A. Identify privileged access rights associated with each system, e.g. operating system, database and application B. Privileged access rights should: - Be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy , i.e. the minimum requirement for their functional role only when needed - Not be granted until the authorization process is complete - Be assigned to a different User ID than the User ID used for day to day work. Regular user activities should not be performed from privileged accounts C. An authorization process and a record of all privileges allocated should be maintained; D. Requirements for expiry of privileged access rights should be defined E. The competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties	●	●	●	

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				F. Specific procedures should be established and maintained in order to avoid the use of generic administration User IDs, according to systems configuration capabilities G. For generic administration User IDs, the confidentiality of security credentials should be maintained when shared (changing them frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms)				
T5.2.3	User Security Credentials Management	P1	Based On Risk Assessment	The entity shall control the allocation of user security credentials. 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	●	●		
T5.2.4	Review Of User Access Rights	P1	Based On Risk Assessment	The entity shall review users’ access rights. C. Authorizations for special privileged access rights should be reviewed at more frequent intervals D. Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained E. Changes to privileged accounts should be logged for periodic review (Please refer document)	●	●	●	

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T5.3	User Responsibilities			Abuse of system access and/or privileges. Management of PASSWORD/CREDENTIAL SECURITY and management.	●	●	●	
T5.3.1	Use Of Security Credentials	P1	Based On Risk Assessment	All users should be advised to: A. Keep secret authentication confidential, ensuring that they are not divulged to any other parties, including people of authority; B. Avoid keeping a record (e.g. paper, software file or hand-held device- of security credentials, unless this can be stored securely and the method of storing has been approved (e.g. password vault); C. Change security credentials whenever there is any indication of their possible compromise; D. When passwords are used as security credentials, select quality passwords with sufficient minimum length which are: 1) Easy to remember 2) Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.; 3) Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries) 4) Free of consecutive identical, all-numeric or all-alphabetic characters E. Change temporary passwords at the first log-on F. Not share individual user's security credentials G. When passwords are used as security credentials in automated logon procedures, these should not be stored without proper protection H. Not use the same security credentials for business and non-business purposes	●	●		
T5.4	Network Access Control			Unauthorized access to network services by internal or external user	●	●		
T5.4.2	User Authentication For External Connections	P1	Based On Risk Assessment	The entity shall: 1) Require all remote login (users and administrators) to be done over secure channels 2) Ensure appropriate authentication methods to be used to control	●	●		

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				access by remote users 3) Block access to a machine (either remotely or locally) for administrator-level accounts				
T5.5	Operating System Access Control			• Abuse of system access/privileges • Backdoor or Command and Control • Disable or interfere with security controls • Tampering in network utilities	●	●		
T5.5.1	Secure Log-On Procedures	P1	Based On Risk Assessment	A. Not display system or application identifiers until the log-on process has been successfully completed B. Display a general notice warning that the computer should only be accessed by authorized users C. Not provide help messages during the log-on procedure that would aid an unauthorized user D. Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect E. Protect against brute force log-on attempts F. Log unsuccessful and successful attempts G. Raise a security event if a potential attempted or successful breach of logon controls is detected; H. Display the following information on completion of a successful log-on 1- Date and time of the previous successful log-on 2- Details of any unsuccessful log-on attempts since the last successful log-on I. Not display a password being entered J. Not transmit passwords in clear text over a network K. Terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the entity's security management or on mobile devices L. Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access Connection time controls should be considered for sensitive	●	●		

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
				computer applications, especially from high risk locations, e.g. public or external areas that are outside the entity's security management. Examples of such restrictions include: A. Using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration B. Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation C. Considering re-authentication at timed intervals				
T5.5.3	User Credentials Management System	P1	Based On Risk Assessment	The user credential management system 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	●	●		
T5.5.4	Use Of System Utilities	P1	Based On Risk Assessment	The entity shall: 1) Identify the system utilities and identify the respective appropriate level of protection 2) Keep track of the user's access rights provided to the system utilities 3) Restrict use of utility programs only to authorized personnel 4) Monitor the use of utility programs			●	
T5.6	Application And Information Access Control			• Unauthorized access by internal or external user • Backdoor or command and control	●	●		
T5.6.1	Information Access Restriction	P1	Based On Risk Assessment	The entity shall: 1) Ensure access to information and application system functions is restricted 2) Ensure access restriction is based on user's roles and responsibilities 3) Assign the appropriate level of access rights to information and application functions 4) For each user and support personnel, adjust their access control based on specific business needs	●	●	●	

Third Party Security

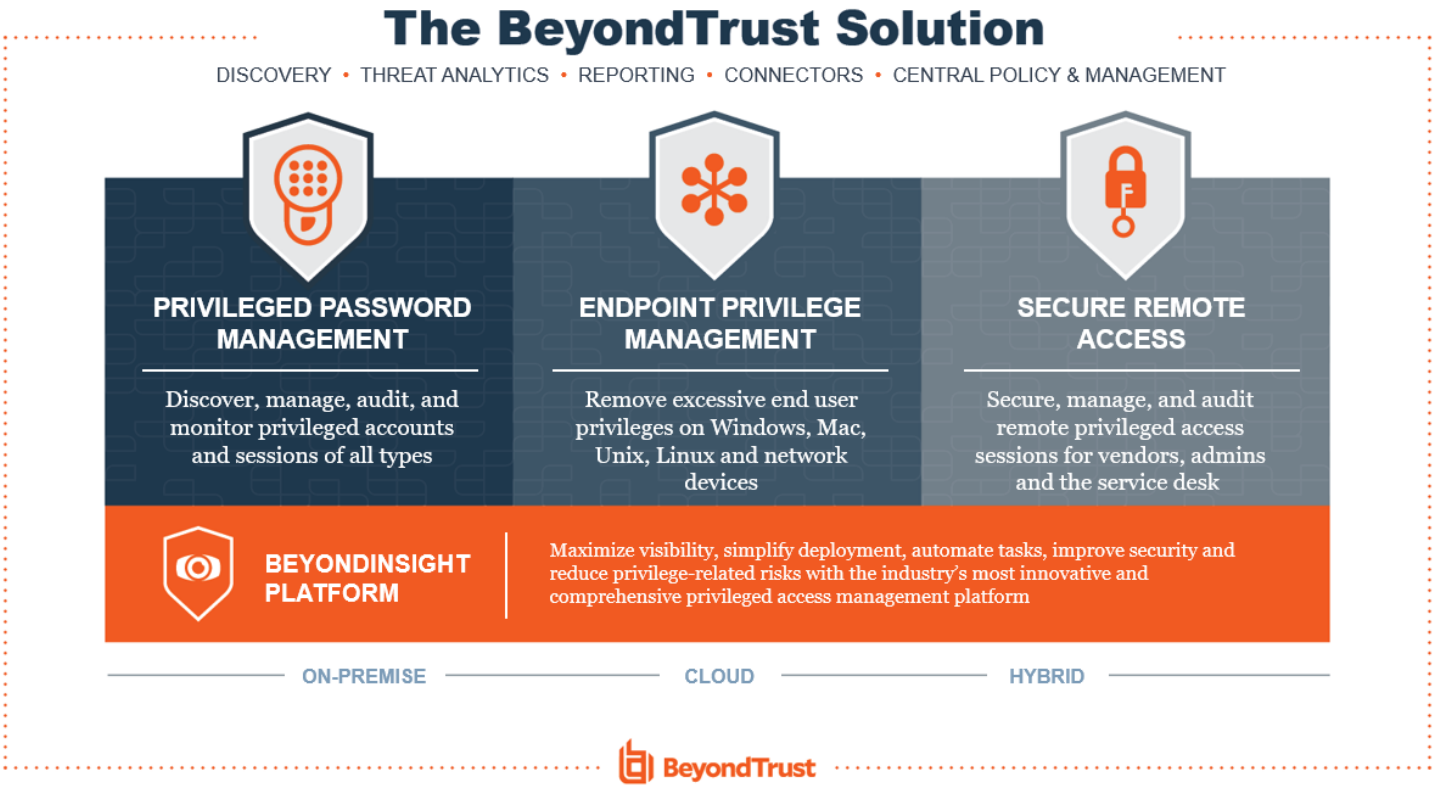
Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T6	Third Party Security			Control, Monitor and audit third party access	●	●		
T6.1	Third Party Security Policy			To maintain a third-party security policy covering the security of acquired services	●	●		
T6.2	Third Party Service Delivery Management			• Abuse of functionality • Data from untrustworthy sources	●	●		
T6.3	Cloud Computing			• Abuse of functionality • Accidental leaks / sharing of data • Illegal processing of data	●	●	●	

Information Systems Acquisition, Development And Maintenance

Control Number	Control Name	Priority	Applicability	Policy Statements To Note	PPM	SRA	EPM	DSS
T7	Information Systems Acquisition, Development And Maintenance			To prevent information misuse or unauthorized modification and to elevate security levels in applications	●		●	●
T7.4	Cryptographic Controls			• Weak keys used for sensitive data	●		●	●
T7.5	Security Of System Files			• Unauthorized access to system files • Corruption of data				●
T7.5.1	Control Of Operational Software	P4	Based On Risk Assessment	The entity shall: 1) Allow the installation of software only by authorized administrators 2) Inhibit installation of software by users, unless justified by their role/ business need				●
T7.5.2	Protection Of System Test Data	P3	Based On Risk Assessment	The entity shall: 1) Use sample data sets to test data applications 2) Limit the transfer of real data from production environment to the test environment, and to be done only after the appropriate authorization	●	●	●	
T7.6	Security In Development And Support Processes			• Unsuitable security for development and support processes • Lack of proper technical review of applications after operating system changes				●
T7.6.3	Restrictions On Changes To Software Packages	P2	Based On Risk Assessment	The entity shall: 1) Define who is entitled to approve changes to software/applications				●

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions. BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace. By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

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.