WHITE PAPER

Satisfying your UAE Information Assurance Standards (UAE IAS) Requirements with One Identity Solutions

> ***"For many organizations, compliance with information security standards doesn't seem to be getting easier. IT security-compliance efforts often compete for money and attention with IT security threats, operational vulnerabilities and daily business risks, and they often lose."***

Introduction

For many organizations, compliance with information security standards doesn't seem to be getting easier. IT security-compliance efforts often compete for money and attention with IT security threats, operational vulnerabilities and daily business risks, and they often lose.

However, the reality is that these areas do not have to compete. By implementing proven solutions that address multiple foundational controls, you can achieve and prove regulatory compliance while guarding against the risks that threaten everyday operations or even land organizations in the headlines. For example, a key component of regulatory compliance is implementing – and demonstrating that you have implemented – reasonable and appropriate IT-related internal safeguards that minimize the risk of unauthorized disclosures and data breaches. Achieving and proving your compliance with such mandates requires you to effectively manage user identities and entitlements. Mitigating the security risk of privileged access to systems and data can satisfy multiple control objectives and enhance your organization's broader security goals.

In this paper, you'll learn about how One Identity can help organizations to address IT security compliance for UAE Information Assurance Standards created by the National Electronic Security Authority (NESA) – also referred to as NESA UAE information assurance standards.

The NESA UAE Information Assurance Standards

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.

One Identity solutions help organizations control user access to enterprise applications and unstructured data in their production operating environments.

The benefits of this technology adoption, however, comes 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 cybersecurity threats and ensuring the development of a secure national information and communications infrastructure is a strategic priority for the UAE. To this end, the NESA UAE information assurance standards is 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 NESA UAE information assurance 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

Moreover, 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

Satisfying Compliance with One Identity's Solutions

One Identity solutions are designed to unify user identities, simplify the user provisioning and deprovisioning process, and provide privileged governance (through authorization, attestations and privilege history) across enterprise applications to the platforms and environments that support critical applications and house sensitive data. In doing so, they fill a critical security gap for traditionally weak IT controls. In addition, these solutions enable organizations to identify sensitive data and enforce security policies that control access to that data user-risk rankings based on data sensitivity, granted privileges and policy violation history can also be applied where needed to provide even more depth to an organizations security controls.

By ensuring controlled access based on need-to-know and providing a detailed history of when authorizations to access account data were granted and by whom, One Identity solutions help organizations control user access to enterprise applications and unstructured data in their production operating environments, thus ensuring that critical access controls are applied to security architectures in all phases of the system development lifecycle.

One Identity solutions discussed in this paper in relation to UAE IAS requirements include the following:

- Identity Manager
- Safeguard Privileged Access Management

1. Identity Manager

In most organizations, IT bears the burden of determining whether a user's access requests should be granted, even though the information needed to avoid potential compliance violations may not be known. Ideally these tasks should be delegated to the business users who understand the context of the requests. To securely move access request, approval and attestation to end users and their managers, strong assurances and parameters need to be established to ensure that all actions and requests are fulfilled in a safe and secure manner.

Identity Manager is an Identity Governance and Administration (IGA) platform that streamlines the access governance process of managing user identities, privileges and security enterprise-wide while providing foundational IT security measures. Identity Manager enables organization to achieve such governance by:

- Consolidating and unifying user identities across the enterprise
- Automating the enforcement of access management, including requests, reviews, approvals, denials, attestations and revocations.
- Identifying risk factors to track users with access to account data and assign risk levels based on risk criteria: e.g. days in current role (without role change) and policy violation history
- Responding to management and audit inquiries with reports that demonstrate historical compliance with many information security policies and procedures
- Monitoring and reporting on active and historical privileges granted, including those with reporting period, system clock or time stamp edit privileges during sensitive time periods or outside the course of normal business operations
- Substantiating evidence of policy violations, such as those involving conflicts of interest.

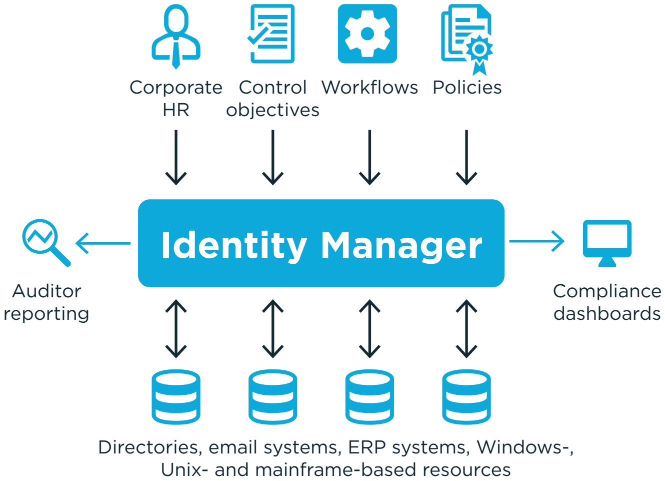


Fig 1: Identity Manager provides a unified solution, simplifying the complex problems of identity & access management

One Identity Manager provides:

Access Governance – Enable business managers to understand what is in the environment and who has access to it, while ensuring that every individual has only the right access to do their job, nothing more.

> ***Privileged Access Governance:*** *Privileged Account Governance enables One Identity Manager customers to integrate their PAM technologies into Identity Manager to support user account provisioning and access governance across the enterprise with complete visibility, while continuing to use comprehensive privilege account, access and session management.*

Application governance - A business view of application entitlements enables a business owner to manage the user lifecycle for each application. Delivers a way to decouple the technical, target-system-driven view from business-centric view. A framework where application owners can manage the applications and entitlements and at the same time prove each of their application is under governance and in compliance. Built-in Key Performance Indicators (KPIs) application owners maintain compliance and compare it against their organization objectives.

Full Visibility and Control – Easily access a clear view of all connected systems and applications, including user entitlements and the status of requests, using a management-friendly dashboard.

Role-based Delegation – Share views with any approved contributor, and limit the data displayed according to their role within the organization.

Rich Auditing and Reporting – Create detailed and professional-looking reports and workflows with ease using out-of-the-box reports and the GUI driven report creator – no coding required. One Identity Manager also has powerful built-in auditing tools.

Time Trace and Change Simulation – Track every object, process, change and action performed and see exactly what was changed, how, by whom and when. A simulation mode exposes the impact of any change before it goes into production and identifies all affected objects, users, rules and system processes, including those that touch connected systems.

Automated Enterprise Provisioning – automatically provision to any system, platform or application using configuration rather than customization.

Self-Service Lifecycle Identity Management – Enable non-IT users to provision accounts, physical assets and control access rights and permissions, with an intuitive and easy-to-use "shopping cart" interface.

Visionary Architecture – Eliminate the typical barriers associated with adopting an Identity & Access Management framework solution with a streamlined, business optimized and rapidly deployed configuration process, instead of an expensive, time-consuming, and complex custom project.

Complements Existing Investments – Support other systems, including "traditional" IAM frameworks. This enables you to plug functionality gaps and make the most of multiple best-in-classsolutions Such as SAP, ServiceNow and more.Business Process Management – Create workflows and attestations based on your business and policy needs. This maximizes security and compliance while eliminating common IAM inefficiencies and redundant processes.

Compliance-ready Identity & Access Management – Achieve and maintain compliance with on-going governance, using your own security policies. With complete visibility into your identities and their access, you'll be able to address the cause of problems rather than the symptom.

2. Safeguard Privileged Access Management

One Identity Privileged Access Management (PAM) solutions mitigate security risks and enable compliance. The Safeguard suite of PAM solutions enables organizations to secure, control, monitor, analyze and govern privileged access across multiple environments and platforms. The focus of Safeguard platform is to provide organizations with a cost-effective modular platform from which can enable various privilege control functions as required based on current or future privileged access control requirements. The key privileged control functions offered under Safeguard include:

Privileged Password Management: Safeguard for Privileged Passwords automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. It ensures that privileged access is granted according to established policies with appropriate approvals; that all actions are fully audited and tracked; and that passwords are changed immediately upon their return.

Safeguard for Privileged Passwords also eliminates the security exposure posed by embedded privileged passwords required for applications to talk to each other or to database by replacing these hard-coded passwords with programmatic calls that dynamically retrieve the account credential.

Privileged Session Management: From remote vendors to developer access to production or other privileged access requirements, the ability to control access, audit access, monitor access and record access is becoming more critical as companies converge internal resources and outsource. Privileged Session Management provides full session management and controls including fine-grain resource access control, active session monitoring and full session recording in an unmatched size efficient format for future replay. Extensive session proxy types supported including: SSH, RDP, Http/Https, MS SQL, Citrix ICA, VMware Horizon View, Telnet, wVNC, x5250, and more.

Enterprises today are being forced to do more with less resources. As a result, the need to provide restricted, controlled and delegated privileged access to internal resources is growing. The unique configurable content alerting and blocking capabilities of Privileged Session Management privileged access control down to command level. Not only are you able to control, record and monitor sessions —you can limit a user's connection to a specific command for both Unix/Linux and Windows systems. This can be used in either a command white listing or blacklisting context.

Privileged Behavior Analytics: Safeguard for Privileged Analytics monitors questionable behaviors and uncovers previously unknown threats from inside and outside of your organization. By using user behavior analytics technology, Safeguard for Privileged Analytics detects anomalies and ranks them based on risk so you can prioritize and take appropriate action -- and ultimately prevent data breaches.

Delegation/Least Privilege Access: provides granular delegation of the Active Directory Administrator account and central control of administrative access using a single, well-defined set of roles, rules and policy. For Unix/Linux environments, centralized management of Sudo and the

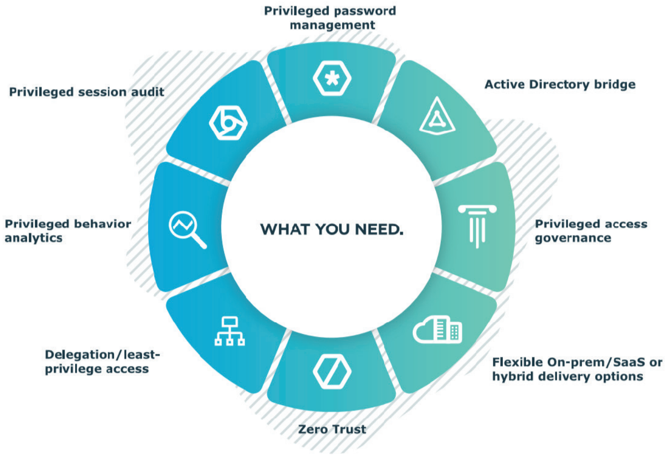

Privileged password management
Active Directory bridge
Privileged access governance
Flexible On-prem/SaaS or hybrid delivery options
Zero Trust
Delegation/least-privilege access
Privileged behavior analytics
Privileged session audit
WHAT YOU NEED.

Fig 2: Safeguard suite of privileged access management solution with comprehensive use-case coverage and easy path to privilege governance

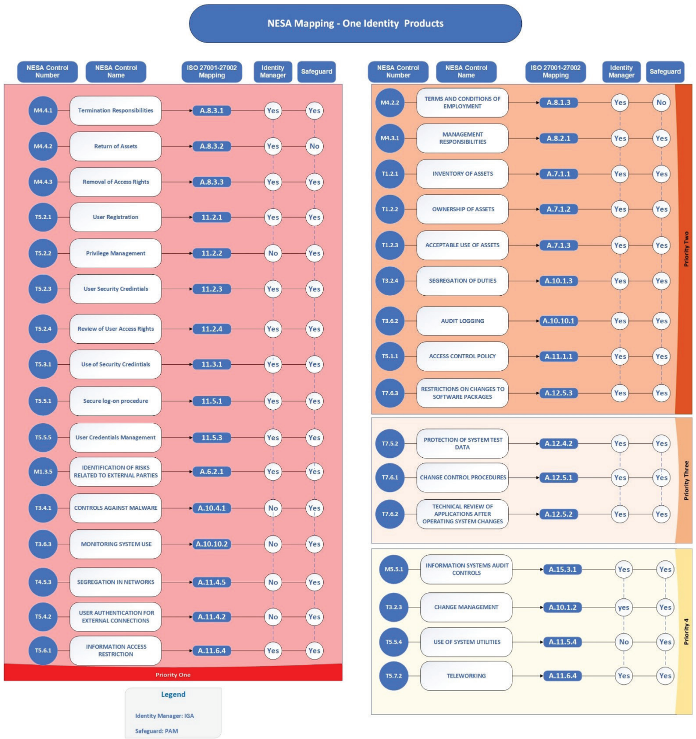
Sudoers policy file, centralized reporting on sudoers access rights and activities – eliminating the box-by-box management of Unix estate. In addition, Privilege Manager for Windows grants user accounts the least privileges necessary according to best practices, yet elevates specific applications as needed. It enables you to control the elevated permissions for desktop users as part of your organization's privileged access management program.

Active Directory Bridge: enhances Safeguard for Sudo by unifying UNIX/Linux identities into Microsoft Active Directory, enabling you to use a common management interface and policy set to control delegation of UNIX root.
Safeguard Authentication Services centralizes authentication and provides single sign-on for UNIX/Linux unifying identities and consolidating directories simplifying management and easing compliance.

Zero Trust: Refer One Identity Zero Trust solutions page to learn how our integrated solution enables Zero Trust using an integrated solution approach.
https://www.oneidentity.com/solutions/zerotrust/

One Identity Solutions Capabilities Mapping with UAE Information Assurance Standards

A. Summary of Controls Mapping



NESA Mapping - One Identity Products

NESA Control Number	NESA Control Name	ISO 27001-27002 Mapping	Identity Manager	Safeguard
M4.4.1	Termination Responsibilities	A.8.3.1	Yes	Yes
M4.4.2	Return of Assets	A.8.3.2	Yes	No
M4.4.3	Removal of Access Rights	A.8.3.3	Yes	Yes
T5.2.1	User Registration	11.2.1	Yes	Yes
T5.2.2	Privilege Management	11.2.2	No	Yes
T5.2.3	User Security Credintials	11.2.3	Yes	Yes
T5.2.4	Review of User Access Rights	11.2.4	Yes	Yes
T5.3.1	Use of Security Credintials	11.3.1	Yes	Yes
T5.5.1	Secure log-on procedure	11.5.1	Yes	Yes
T5.5.5	User Credentials Management	11.5.3	Yes	Yes
M1.3.5	IDENTIFICATION OF RISKS RELATED TO EXTERNAL PARTIES	A.6.2.1	Yes	Yes
T3.4.1	CONTROLS AGAINST MALWARE	A.10.4.1	No	Yes
T3.6.3	MONITORING SYSTEM USE	A.10.10.2	No	Yes
T4.5.3	SEGREGATION IN NETWORKS	A.11.4.5	No	Yes
T5.4.2	USER AUTHENTICATION FOR EXTERNAL CONNECTIONS	A.11.4.2	No	Yes
T5.6.1	INFORMATION ACCESS RESTRICTION	A.11.6.4	Yes	Yes

Priority One

Legend

Identity Manager: IGA

Safeguard: PAM

NESA Control Number	NESA Control Name	ISO 27001-27002 Mapping	Identity Manager	Safeguard
M4.2.2	TERMS AND CONDITIONS OF EMPLOYMENT	A.8.1.3	Yes	No
M4.3.1	MANAGEMENT RESPONSIBILITIES	A.8.2.1	Yes	Yes
T1.2.1	INVENTORY OF ASSETS	A.7.1.1	Yes	Yes
T1.2.2	OWNERSHIP OF ASSETS	A.7.1.2	Yes	Yes
T1.2.3	ACCEPTABLE USE OF ASSETS	A.7.1.3	Yes	Yes
T3.2.4	SEGREGATION OF DUTIES	A.10.1.3	Yes	Yes
T3.6.2	AUDIT LOGGING	A.10.10.1	Yes	Yes
T5.1.1	ACCESS CONTROL POLICY	A.11.1.1	Yes	Yes
T7.6.3	RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES	A.12.5.3	Yes	Yes

Priority Two

NESA Control Number	NESA Control Name	ISO 27001-27002 Mapping	Identity Manager	Safeguard
T7.5.2	PROTECTION OF SYSTEM TEST DATA	A.12.4.2	Yes	Yes
T7.6.1	CHANGE CONTROL PROCEDURES	A.12.5.1	Yes	Yes
T7.6.2	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING SYSTEM CHANGES	A.12.5.2	Yes	Yes

Priority Three

NESA Control Number	NESA Control Name	ISO 27001-27002 Mapping	Identity Manager	Safeguard
M5.5.1	INFORMATION SYSTEMS AUDIT CONTROLS	A.15.3.1	Yes	Yes
T3.2.3	CHANGE MANAGEMENT	A.10.1.2	yes	Yes
T5.5.4	USE OF SYSTEM UTILITIES	A.11.5.4	No	Yes
T5.7.2	TELEWORKING	A.11.6.4	Yes	Yes

Priority 4

Fig 2: Safeguard suite of privileged access management solution with comprehensive use-case coverage and easy path to privilege governance

***Zero Trust:** Refer One Identity Zero Trust solutions page to learn how our integrated solution enables Zero Trust using an integrated solution approach.*

B. Description of How One Identity Solution Satisfies the Requirements

M1.3.5 - IDENTIFICATION OF RISKS RELATED TO EXTERNAL PARTIES	P1
CONTROL	The entity shall identify and properly manage the risks related to its information and information systems from business processes involving external parties
SUB-CONTROL	The entity shall: 1) Identify risks to its information and information systems and implement the appropriate controls before granting access to any external party 2) Define an external party access policy 3) Identify and adopt proper controls to limit physical and logical access to information assets and entity information systems 4) Monitor external party access to entity information and entity information systems
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager can be used to provision custom objects such as accounts on smart phones, tablets and remote access VPNs. In addition, these solutions can manage the assignment of identities and privileges on servers and applications that IT uses to manage mobile devices and remote access users to ensure mobile device and VPN administrator activities are properly authorized, traceable to specific users and conform to the organization's mobile device and remote access policies. **PAM:** Organizations allowing remote access need a policy that restricts remote access privileges. Safeguard PAM can restrict unauthorized remote IP addresses for API and CLI sessions. Safeguard automatically generate randomized passwords to reduce the risk of pass-the-hash, credential harvesting and other exploits that are often associated with remote access. And Safeguard for Privileged Sessions also protects against viruses, malware and other dangerous items that may exist on a remote user's system because it proxies all sessions to target resources. In addition, it records all actions users perform.

M4.2.2 - TERMS AND CONDITIONS OF EMPLOYMENT	P2
CONTROL	The entity shall ensure that employees, contractors and third-party user understand, agree and sign the terms and conditions of their employment contract, which should state their and the entity's responsibilities for information security, as part of their contractual obligation
SUB-CONTROL	The entity shall: 1) Define standard information security terms and conditions for employees, third parties and contractors 2) Include information security terms and conditions in any contract 3) Ensure that their employees, contractors, and third parties fully understand their relevant terms and conditions 4) Review and eventually amend any existing contract with employees, contractors and third parties
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager enable you to establish and enforce access authorization to systems that store, process or transmit legally protected and confidential information thereby limiting access to not only those individuals whose job requires such access, but to only those have successfully passed a background check and have a need to know. Specifically, these solutions are designed to: • Define access needs across enterprise applications, NTFS, NAS devices and SharePoint servers for each role, including file servers and data resources that each role needs to access for their job function • Restrict user access to least privileges necessary to perform job responsibilities • Put user access administration into the hands of appropriate authority personnel to delegate access granting privileges and manage entitlement creep for on-going maintenance of access restrictions • Support policies requiring authority personnel to assign, periodically review and attest to the legitimacy of access privileges based on individual personnel's job classification and function. • Support policies requiring documented approval by authorized parties specifying required privileges and/or approving access requests. • Establish access control for systems with multiple users that restricts access based on a user's need to know • Ensure that access controls (e.g. rules and policies) equivalent to default "deny all" configurations are in place for all system components with multiple users • Provide a full-featured model for the complete management and review of user identities and access rights

M4.3.1 - MANAGEMENT RESPONSIBILITIES	P2
CONTROL	The entity’s management shall require employees, contractors and third-party users to apply security in accordance with established policies and procedures of the entity.
SUB-CONTROL	The entity shall: 1) Include in human resources security policy that employees, contractors and third-party users have to comply with entity security policies and procedures 2) Inform all employees, contractors and third parties of the security policies they are required to be compliant with 3) Present, on first access, relevant security policy/guidelines for users to read and accept
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA & PAM:** Deploying Identity Manager & Safeguard provides an excellent way for management to demonstrate its support of the organization’s information access policies and procedures by enforcing them.

M4.4.1 - TERMINATION RESPONSIBILITIES	P1
CONTROL	The entity shall clearly define and assign responsibilities for performing employment termination or change of employment.
SUB-CONTROL	The entity shall: 1) Define an employee termination policy that emphasizes the communication of termination responsibilities in relation to entities information security (including confidentiality and property rights) 2) Assign responsibility for performing termination or change of employment

M4.4.1 - TERMINATION RESPONSIBILITIES	P1
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager is designed to manage the information security aspects of employee and contractor terminations and job reassignments (such as orphaned accounts) by quickly terminating access privileges to sensitive information and reducing or removing access to system accounts — even if a user has multiple identities from holding different roles over many years with the organization. Identity Manager enables you to adjust or revoke system access privileges across your ERP system, NTFS, NAS devices and SharePoint servers in a timely manner for workforce members who have changed roles or have left the organization. Moreover, with Identity Manager you can easily review and remove or disable inactive user accounts across all these systems and monitor for orphaned accounts in accordance with your organization's account aging policy. **PAM:** Safeguard can quickly terminate access privileges to sensitive information and reduce or remove access to system accounts — even if a user has multiple identities from holding different roles over many years with the organization.

M4.4.2 - RETURN OF ASSETS	P1
CONTROL	The entity shall ensure that all stakeholders should return all of the entity's assets in their possession upon termination of their employment, contract or agreement.
SUB-CONTROL	The entity shall: 1) Include in employee termination policy that all employees, contractors and third parties should return of all assets upon termination of employment, contract or agreement
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager can manage both logical and physical assets assigned to employees. Upon termination of employment, Identity Manager can automatically de-provision all the logical access of the employees. Identity Manager can alert the asset owners to ensure that the required physical assets are returned. Alternatively, the Identity Manager can be integrated with the helpdesk systems to raise a ticket for fulfillment.

M4.4.3 - REMOVAL OF ACCESS RIGHTS	P1
CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	The Identity Manager provide organizations with a ready-made framework designed to inherit and/or set up, manage and support: • User authentication information • A formal user registration and de-registration process to enable assignment of access rights • A formal user access provisioning process to assign or revoke access rights for all user types to all systems and services • A full-featured model for the complete management and review of access rights Identity Manager enable organizations to implement access authorization, access rights review and access revocation policies for granting and maintaining least-privilege access to sensitive data across a variety of platforms. Features include the assignment of unique user IDs; the means to review and adjust or revoke system access privileges across ERP, NTFS, NAS devices and SharePoint servers in a timely manner for users who have changed roles or have left the organization; and the assured elimination of redundant user IDs across multiple platforms through a secure, centralized repository for user credentials. **PAM:** Safeguard provides organizations with means to revoke system access privileges across a variety of platforms in timely manner.

M5.5.1 - INFORMATION SYSTEMS AUDIT CONTROLS	P4
CONTROL	The entity shall ensure that audit requirements and activities involving checks on operational systems are carefully planned and agreed to minimize the risk of disruptions to business processes.
SUB-CONTROL	The entity shall: 1) Assign responsibilities for internal audits of information system controls to an appropriate authority 2) Define audit requirements for information system controls 3) Outline an audit plan to meet audit requirements for information system controls 4) Highlight measures taken to ensure audit activities minimize the risk of disruptions to business processes
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager offer many evidences (granted permissions, logs, reports, configuration settings, security rule violations) that indicate the extent the organization has met identity and access management audit controls. Identity Manager can also be used to assign a risk value to every company resource identified in Identity Manager. A risk index is then calculated for every user assigned to a risk-rated resource. Security rules too can be assigned a risk value for audit purposes so that a user's rule violations affects his or her risk index. A user's risk index can be further refined through various attributes including a user's assigned roles and responsibilities. This provides audit teams with the ability to focus on higher risk areas that can be audited by user and by system. **PAM:** Safeguard can provide audit teams with timed, recorded, scope-bounded, read-only privileges to session recordings, enabling them to audit privileged activities in many information systems that contain or provide access to sensitive information. Privileged activities can be audited by user and by system.

T1.2.1 – INVENTORY OF ASSETS	P2
T1.2.2 – OWNERSHIP OF ASSETS	P2
T1.2.3 – ACCEPTABLE USE OF ASSETS	P2

HOW ONE IDENTITY SATISFIES THE REQUIREMENTS

IGA: Identity Manager can identify critical technology assets and personnel (with contact information) associated with your organization’s ERP system, NTFS systems, NAS devices and SharePoint servers. In fact, One Identity’s IAM solution provides a number of features that can help you inventory critical technology assets and determine device owner information. For example, to augment the usage restrictions that are configured during user account setup, usage policies can be established with rules for when and how user accounts can access system components. Once established, reports such as the Resource Activity Report can provide a list of all access activity on those critical technologies, the personnel authorized to use the devices and whether usage policies have been violated. The Identity Manager can ensure that only asset owners or those authorized by asset owners can grant access privileges to specific assets (i.e. to only those areas, applications and functions required for assigned tasks) and provides centralized reporting for all access violations on Windows file servers, SharePoint and NAS devices.

PAM: Safeguard can automatically discover all systems in your organization’s directory and export a list of active systems associated with the appliance, in either Excel or CSV format.

Safeguard can ensure that only asset owners or those authorized by asset owners can grant access privileges to specific assets.

Safeguard can enforce a policy requiring that access privileges be granted to only those areas, applications and functions required for assigned tasks.

T3.2.3 - CHANGE MANAGEMENT	P4
CONTROL	The entity shall control the changes to information systems.
SUB-CONTROL	The entity shall: 1) Document a change management process 2) Integrate specific process controls to ensure the change management process is executed correctly 3) Define the systems to which the change management process applies 4) Assign management responsibilities for control of changes to identified systems
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Changes management is a foundational control for keeping unauthorized changes out of production operating environments. Identity Manager provide a full-featured access governance solution that can enforce change approval processes in both development and production environments including the access controls needed during data migrations. **PAM:** Safeguard can enforce change approval processes in both development and production environments. In addition, these tools are ideal for emergencies, when quick (but controlled) changes are required to resolve an incident.

T3.2.4 - SEGREGATION OF DUTIES	P2
CONTROL	The entity shall segregate duties and areas of responsibility.
SUB-CONTROL	The entity shall: 1) Identify specific sets of duties that should be segregated 2) Ensure duties with segregation requirements are assigned to different resources 3) Implement suitable alternative controls in the case that duties with segregation requirements cannot be assigned to different resources
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager support the enterprise-wide access control and access management requirements that are part of every information security policy. In particular, these tools help ensure that policies addressing role assignments, including information security management entitlements and segregation of duty (SoD) requirements are defined and enforced across your network. In addition, Identity Manager can support the information security policy review process.

T3.2.4 - SEGREGATION OF DUTIES	P2
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** Safeguard help ensure that authorization and separation of duty (SoD) requirements are defined and enforced across all platforms in your network. Safeguard retrieves and checks user credentials, group memberships and level of privileges based on their Active Directory account when authenticating privileged users. Safeguard can create rule sets to blacklist console commands and activities to mitigate malicious activities, misuse and potential security threats. It can also restrict or prohibit entry via specific ports and protocols.

T3.4.1 - CONTROLS AGAINST MALWARE	P1
CONTROL	The entity shall protect its information assets from malware.
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** The Safeguard solutions greatly reduce the risk of malware spreading in your network. For example, these solutions can restrict, manage and monitor activities in which malicious software is known to infect a network, such as new software downloads, automated software updates and unauthorized software installations. In addition, enhance security by limiting access to the desktop admin account and privileged applications. Safeguard monitors the network traffic in real-time and executes various actions if a certain pattern appears on the screen. In case of detecting a suspicious user action, Safeguard can send out an email alert or immediately terminate the connection.

T3.6.2 - AUDIT LOGGING	P2
CONTROL	The entity shall produce and keep audit logs recording user activities, exceptions, and information security events.
SUB-CONTROL	The entity shall: 1) Identify all activities to be captured in audit logs for all hardware devices, operating systems and installed applications 2) Identify minimum information requirements for each activity to be captured 3) Define minimum frequency requirements for reviewing audit logs 4) Ensure audit logs are reviewed by personnel with appropriate training and skills 5) Define minimum time requirements for maintaining audit logs

T3.6.2 - AUDIT LOGGING

P2

HOW ONE IDENTITY SATISFIES THE REQUIREMENTS

IGA: Identity Manager provide a number of logging and monitoring capabilities. For example, Identity Manager can be configured to alert appropriate personnel via email or text message for any specified number of repeated failed logins. The solution can also be used in a review capacity that supports monitoring of login attempts. Identity Manager enable you to limit viewing access of system logs to only those individuals whose job requires such access and have a job-related need.

Identity Manager includes process monitoring functionality that permits authorized persons to configure change tracking methods that monitor changes made in Identity Manager. These methods can be used to monitor all user actions if needed. Change history in Identity Manager can be tracked in at least three ways:

- Logging changes to data (operations on objects)
- Logging process information (ID, action, user, time, etc.)
- Logging messages in the process history

Change history is saved in the Identity Manger database and transferred at regular intervals, or exported as XML files, into a history database. Log files can be stored in specified secured directories and copied, if needed, to a secure system outside the control of a system administrator or operator. Historical data is evaluated using Identity Manager's TimeTrace function.

PAM: Safeguard can provide audit teams with timed, recorded, scope-bounded, read-only privileges to session recordings, enabling them to audit privileged activities in many information systems that contain or provide access to sensitive information. Privileged activities can be audited by user and by system.

Safeguard protect logging facilities and log information in at least three ways:

- By permitting only authorized administrators to access them
- By creating its own record of sensitive privileged sessions to supplement the information contained in event logs
- By keeping a record of all authorized access to event logs

In addition, the appliance has its own database event log, logon security log, firewall log, Proc log (which collects information on cluster replication, software updates, batch processing and system services), alert log and archive log. It also gives you the option of securely replicating system admin, user activity and failed login events to a non-destructive syslog server.

T3.6.3 - MONITORING SYSTEM USE

P1

CONTROL	The entity shall monitor the use of information systems

T3.6.3 - MONITORING SYSTEM USE	P1
SUB-CONTROL	The entity shall: 1) Identify all types of system use to be monitored 2) Identify minimum information gathering requirements for each monitoring activity 3) Define minimum frequency requirements for reviewing information gathered from monitoring activities 4) Ensure information gathered from monitoring activities is reviewed by personnel with appropriate training and skills 5) Define minimum time requirements for maintaining information gathered from monitoring activities
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** Safeguard can monitor privileged users in real-time when connecting to critical assets. All activities are recorded and stored in movie like audit trails. It can also white and blacklist commands and activities to mitigate malicious activities, misuses and potential security threats. Safeguard's 4-eyes or Dual-control authorization allows to oversee and control what privileged users do when accessing critical assets. Privileged users can access critical assets only if authorized by someone operating SPS. The feature allows to real-time observe the session or later review it in a movielike audit trail format. In the event of any misuses or harmful activity the session can be terminated. Safeguard detects abnormal privileged user behavior by comparing a privileged user's constructed profile to their real-time actions. The profile records: • Level of privileges • User's IP address • On average the user's time of access and session duration • Most frequently used console commands • Most frequently accessed cyber assets • Mouse movement and keystroke dynamics If the difference between the two compared items exceeds the tolerance threshold, it will be indicated as abnormal behavior. Safeguard generates logs regarding monitored sessions and behavior analytics that can be consumed and processed by SIEM technologies.

T4.5.3 - SEGREGATION IN NETWORKS	P1
CONTROL	The entity shall segregate groups of information services, users, and information systems on networks.
SUB-CONTROL	The entity shall: 1) Identify criteria for grouping information services, users, and information systems into different groups that facilitate segregation on networks 2) For each group, identify specific segregation requirements 3) Ensure identified segregation requirements are included in the relevant system / service development lifecycle 4) Periodically evaluate the effectiveness of implemented segregation strategies and identify areas for improvement
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** Network segregation is a standard security control for isolating logical groups of servers and users who have similar trust levels or who are working at the same location or in the same department. This prevents network users from having access to all devices in the organization's network from those who generally do not have a need to know. Safeguard is designed to work with popular methods of network segregation, such as subnets, Windows domains and AD forests, to support multiple types of network segregation, such as location-specific, department-specific or domain specific sets of access controls.

T5.1.1 - ACCESS CONTROL POLICY	P2
CONTROL	The entity shall establish an access control policy based on business and security requirements.
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Using the fine-grained access control configuration settings for users, groups, domains, and services, Identity Manager lets you implement the requirements identified in the "implementation guidance" of sections T5.1.1 For example, Identity Manager lets you implement segregation of access control roles, formal authorization of access requests, and mandatory periodic reviews of access rights (attestations) within an Identity Manager network. **PAM:** Likewise, Safeguard can enforce logical access control identified in the "implementation guidance" for privileged access roles.

T5.2.1 - USER REGISTRATION	P1
CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** The Identity Manager provide organizations with a ready-made framework designed to inherit and/or set up, manage and support: • User authentication information • A formal user registration and de-registration process to enable assignment of access rights • A formal user access provisioning process to assign or revoke access rights for all user types to all systems and services • A full-featured model for the complete management and review of access rights Identity Manager enable organizations to implement access authorization, access rights review and access revocation policies for granting and maintaining least-privilege access to sensitive data across a variety of platforms. Features include the assignment of unique user IDs; the means to review and adjust or revoke system access privileges across ERP, NTFS, NAS devices and SharePoint servers in a timely manner for users who have changed roles or have left the organization; and the assured elimination of redundant user IDs across multiple platforms through a secure, centralized repository for user credentials. **PAM:** Likewise applicable to privileged users. In particular privileged account governance (PAG) provides simplified compliance and governance with centralized policy and administration.

T5.2.2 - PRIVILEGE MANAGEMENT	P1
CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** The Safeguard solution ensures that each system user is uniquely identified; the abuse of system accounts is actively being prevented; strong password management settings are enforced; all privileged use activity is being tracked, recorded and logged; audit trails are secured; and explicit approval by authorized parties is required. Authentication to Safeguard and privileged access is augmented with strong authentication as required. Having these foundational IT security measures operating in both development and production environments complements user activity monitoring, malware and intrusion detection controls — providing the necessary layers for the defense in depth approach to information security needed in today's information risk climate.

T5.2.3 - USER SECURITY CREDENTIALS	P1
CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager offers configurable, secure, centralized management of account passwords along with related password QA questions and password change alerts for all users registered in Password Manager, including a self-service password change workflow history which is stored as securely as the passwords themselves: in a centralized password change history safe that is secured using full disk encryption. Identity Manager supports policies for secure initial password distribution, password renewal, password complexity and password change frequency. **PAM:** The Safeguard PAM provide a centralized, secure password vault and password request workflow for authorizing and managing privileged user access controls. All data stored in Safeguard is encrypted in storage and in transit. All connections to remote systems are proxied through the appliance, ensuring a secure single access point. Safeguard supports encrypted communication between privileged users and critical assets via a wide set of protocols, including SSH, RDP, HTTP(s), Citrix ICA.

T5.2.4 - REVIEW OF USER ACCESS RIGHTS	P1
CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** The Identity Manager provide organizations with a ready-made framework designed to inherit and/or set up, manage and support: • User authentication information • A formal user registration and de-registration process to enable assignment of access rights • A formal user access provisioning process to assign or revoke access rights for all user types to all systems and services • A full-featured model for the complete management and review of access rights Identity Manager enable organizations to implement access authorization, access rights review and access revocation policies for granting and maintaining least-privilege access to sensitive data across a variety of platforms. Features include the assignment of unique user IDs; the means to review and adjust or revoke system access privileges across ERP, NTFS, NAS devices and SharePoint servers in a timely manner for users who have changed roles or have left the organization; and the assured elimination of redundant user IDs across multiple platforms through a secure, centralized repository for user credentials. **PAM:** Privileged users can access critical asset upon authorization as controlled by policy. The feature allows to real-time observe the session or later review it in a movie like audit trail format. In the event of any misuses or harmful activity the session can be terminated. Safeguard immediately denies the access of users as soon as their privileges or relevant group memberships are revoked in the central LDAP database. Access to shared accounts or devices that cannot authenticate the user to LDAP is also denied immediately. **PAG:** PAG ensures that privilege account users gain and maintain the appropriate level of access to accounts, while periodic attestations ensure the privileged access is regularly attested and assigned correctly.

T5.3.1 - USE OF SECURITY CREDENTIALS	P1
CONTROL	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)
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** While still widely practiced in the industry, traditional user account/password combinations are fast becoming inadequate when used as the sole means of authenticating users who access business critical systems. To meet the current standard of “reasonable and appropriate” additional authentication safeguards should be considered, including access approval procedures and robust authentication controls such as strong passwords and/or multi-factor authentication. Identity Manager enforces a number of additional authentication safeguards including access approval workflows and self-serve password management that can be configured to implement strong password policies. **PAM:** Safeguard PAM automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. It ensures that privileged access is granted according to established policies with appropriate approvals; that all actions are fully audited and tracked; and that passwords are changed immediately upon their return.

T5.4.2 - USER AUTHENTICATION FOR EXTERNAL CONNECTIONS	P1
CONTROL	The entity shall use appropriate authentication methods to control access of remote users.
SUB-CONTROL	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 access by remote users 3) Block access to a machine (either remotely or locally) for administrator-level accounts

T5.4.2 - USER AUTHENTICATION FOR EXTERNAL CONNECTIONS	P1
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** Safeguard for Privileged Sessions enables authorized trusted workforce members to issue privileged access for a specific period or session to administrators, remote vendors and high-risk users — with full recording and replay for auditing and compliance. It provides a single point of control from which trusted workforce members can authorize connections, limit access to specific resources, allow only certain commands to be run, view active connections, record all activity, alert if connections exceed pre-set time limits, and terminate connections. In addition, One Identity Defender multifactor authentication can further enhance security by enforcing strong authentication to gain access to resources in remote access scenarios.

T5.5.1 - SECURE LOG-ON PROCEDURES	P1
CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager support the secure log-on procedures included with the authentication module selected when setting up or reconfiguring the product (AD, LDAP, local system user or other). Virtually all of these options address most or all of the secure logon procedure requirements such as logon screens and associated logic 1) do not display application or platform software identifiers, 2) have a warning message that only authorized users should access the system, 3) do not provide help that would aid an unauthorized user, 4) do not tell a user which part of a failed logon attempt is incorrect, 5) protect against brute force attempts, 6) log unsuccessful login attempts, 7) raise a security event for failed or successful logon breaches, 8) display details of last successful log-on and unsuccessful logon attempts, 9) obfuscate passwords being entered, 10) render passwords sent over a network unreadable, 11) terminate logon sessions after defined period of inactivity, and 12) restrict connection times for higher risk applications to predefined limits. **PAM:** Safeguard support a wide variety of secure log-on procedures that meet the requirements of the control and implementation guidance.

T5.5.3 - USER CREDENTIALS MANAGEMENT	P1
CONTROL	The entity shall implement a system for managing user credentials (i.e. passwords).
SUB-CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager offers configurable, secure, centralized management of account passwords along with related password QA questions and password change alerts for all users registered in Password Manager, including a self-service password management. Identity Manager supports policies for secure initial password distribution, password renewal, password complexity and password change frequency. **PAM:** The Safeguard solution provide a centralized, secure password vault and password request workflow for authorizing and managing privileged user access controls. Safeguard PAM supports configurable, granular change control of privileged credentials, including time-and last-use-based, and manual or forced change based on organization's policy.

T5.5.4 - USE OF SYSTEM UTILITIES	P4
CONTROL	The entity shall restrict and control the use of utility programs that might be capable of overriding system and application controls.
SUB-CONTROL	The entity shall: 1) Identify the system utilities and identify the respective appropriate level of protection 2) Keep track of the users access rights provided to the system utilities 3) Restrict use of utility programs only to authorized personnel 4) Monitor the use of utility program

T5.5.4 - USE OF SYSTEM UTILITIES	P4
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**PAM:** Safeguard provide a centralized, secure password vault and password request workflow for authorizing and managing privileged user access controls. They also enable you to grant and log temporary use of privileged utility programs across a variety of database and operating system platforms.

T5.6.1 - INFORMATION ACCESS RESTRICTION	P1
CONTROL	The entity shall restrict access to information and application system functions in accordance with the access control policy.
SUB-CONTROL	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
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager restricts access to sensitive information by associating users with permissions groups and through group permission inheritance in AD, SharePoint, and SAP groups. Identity Manager restricts access to sensitive information per your organization's access control policy. Specifically, these solutions enable you to avoid unchecked privileged access and entitlement creep by ensuring authorized personnel carefully review and attest to the validity of user access permissions and grant access to privileged information via an access request/approval workflow. **PAM:** Safeguard can all restrict access to sensitive information (and system functions that could potentially provide such access) per your organization's access control policy. Specifically, these solutions enable you to carefully manage privileged access and grant access to privileged information via an access request/approval workflow.

T5.7.2 - TELEWORKING	P4
CONTROL	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 measure
HOW ONE IDENTITY SATISFIES THE REQUIREMENTS	**IGA:** Identity Manager can be used to provision custom objects such as accounts on smart phones, tablets and remote access VPNs. In addition, these solutions can manage the assignment of identities and privileges on servers and applications that IT uses to manage mobile devices and remote access users to ensure mobile device and VPN administrator activities are properly authorized, traceable to specific users and conform to the organization's mobile device and remote access policies. **PAM:** Organizations allowing remote access need a policy that restricts remote access privileges. Safeguard can restrict unauthorized remote IP addresses for API and CLI sessions. Safeguard automatically generate randomized passwords to reduce the risk of pass-the-hash, credential harvesting and other exploits that are often associated with remote access. And Safeguard for Privileged Sessions also protects against viruses, malware and other dangerous items that may exist on a remote user's system because it proxies all sessions to target resources. In addition, it records all actions users perform.

T7.5.2 – PROTECTION OF SYSTEM TEST DATA	P3
CONTROL	The entity shall ensure the protection of system test data.
SUB-CONTROL	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 3) Erase any data from test applications immediately after testing is completed 4) Keep track of any copy/erase of data between production and testing environment

T7.5.2 – PROTECTION OF SYSTEM TEST DATA	P3

HOW ONE IDENTITY SATISFIES THE REQUIREMENTS

IGA: For test environments containing sensitive operational data, Identity Manager can ensure that:

- The access request procedures that apply to operational application systems also apply to test application systems.
- Special authorization is obtained before accessing test environments containing sensitive data copied from an operational environment.
- Conflicting entitlements are prevented through enforced policy (e.g., users with access authorization to test environments do not have access authorization to environments containing operational data.)

PAM: Safeguard can implement and enforce the privileged access authorization aspects of separating operational, testing, and development environments

T7.6.1 – CHANGE CONTROL PROCEDURES	P3
T7.6.2 – TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING SYSTEM CHANGES	P3
T7.6.3 - RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES	P2

HOW ONE IDENTITY SATISFIES THE REQUIREMENTS

IGA: By facilitating the implementation of identity and access governance principles, Identity Manager can help organizations ensure information security controls are applied in the development lifecycle processes of information systems. For example, these solutions can be used

1) to prevent the common problem of developer accumulation of excess privileges (or “entitlement creep”) by defining how access policy rules are assigned to the various roles in a systems development effort;

2) for establishing the risk levels that will be used for ranking risk during the development process (e.g., based on a developer’s privileges, trustworthiness, and the sensitivity of data being accessed); and

3) for establishing baseline risk thresholds for all objects (e.g., users, roles, groups, rules, and policies).

In addition, they offer a configurable workflow that ensures all appropriate reviews, analysis, testing and production update scheduling is performed before such software is installed.

PAM: Safeguard can implement and enforce the privileged access authorization aspects of separating operational, testing, and development environment.

Safeguard can reduce technical vulnerabilities, such as unauthorized software downloads and installations, by enabling authorized administrators to ensure that all appropriate reviews, analysis, testing and production update scheduling is performed before software is installed.

Conclusion

The One Identity solutions helps organizations achieve an identity-centric security strategy with a uniquely broad and integrated portfolio of identity management offerings. The solutions covered in this paper provide account lifecycle management, identity governance and administration (IGA), and privileged access management (PAM) regardless of the location of resources – on-prem, in the cloud or hybrid. With One Identity solutions, you have access to a business-centric, modular and integrated portfolio, which is virtually non-existent in legacy solutions. Moreover, our identity-centric offering includes AD, IGA and PAM point solutions.

You can consolidate multiple user identities to establish unique user accounts across disparate platforms; you can establish access policies, manage user entitlements, monitor for data access policy violations and maintain related history across all systems even if they natively lack access management capabilities. This powerful solution set closes a fundamental security gap in traditionally weak infrastructure controls.

One Identity solutions, particularly our PAM offering, enables organizations to fulfill a substantial number of UAE IAS reference controls for protecting unauthorized access to virtually all systems within the scope of organization (or UAE IAS scope). In addition to meeting control requirements, you can automate a substantial number of UAE IAS reference controls for protecting unauthorized access to virtually all systems within the scope and delivers a sound return on investment.

About One Identity

One Identity by Quest, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com