Assessing Privileged Access Management (PAM) using ISO 27001:2013 Control

Anton Purba[1], Mohammad Soetomo[2]

[1] Faculty of Engineering and Information Technology, Swiss German University
Kota Tangerang, 15143, Indonesia
anton.purba [at] student.sgu.ac.id
[2] Faculty of Engineering and Information Technology, Swiss German University
Kota Tangerang, 15143, Indonesia
mohammad.soetomo [at] student.sgu.ac.id

Abstract. ISO 27001 is one of the most widely adopted and respected information security standards in use today. It is promulgated by the International Standards Organization (ISO). Many organizations seek to be certified for the standard, which provides a framework for implementing an Information Security Management System (ISMS). The standard touches on virtually every aspect of information security. Access controls - including Privileged Access Management (PAM), thus figure prominently into the ISO 27001 certification and audit processes. In order to manage their privileged accounts, organization should be use PAM to protect critical IT assets, meet the compliance regulation and to prevent data breaches. But unfortunately many organizations do not have enough knowledge when they plan to build PAM solutions. Many organization do not have base-line when they acquire new PAM technology. This paper will help organization to acquire PAM solution that meet the ISO 27001 control. Our compliance matrix give organization a guideline to achieving the implementation of ISMS framework with PAM technology.

1. Introduction

The ISO 27001 standard sets out a specification for the development of an information security management system (ISMS) and guarantees that an organization is following international information security best practices (Itradat *et al.*, 2014). The goal of ISO 27001 is to help organizations set up and maintain effective information security using a process of continual improvement. ISO 27001 provides a control framework for virtually every aspect of information security. The standard has controls devoted to security policy, physical security, incident response and so forth.

Administrative account such as root, administrator, super user and domain admin are all privileged accounts that have unlimited access (Harley and Lee, 2006). User administrator that has access to the system can perform any task using privileged account, and multiple users will use the same account ID and password. Using privileged account roles give them elevated privileges that essentially give users full control over the systems they are managing.

Privileged access is one of the most sensitive aspects of IT. According to Verizon Data Breach 2018, the misuses of privileged account is the 3rd breaches incident on the Public Administration sector (*2018 Data Breach Investigations Report*, 2018). The privileged accounts have the ability to make sweeping

and fundamental changes to IT systems on which the business may depend. When used in unintended ways, their impact can cause a wide spectrum of damage from compliance violations resulting in fines, to security incidents causing reduced brand confidence and lost revenue ('Three Important Reasons for Privileged Identity Management', 2015).

Solution like Privileged Access Management (PAM) can manage privileged access, log all activity in the form of session recordings or keystroke logging, and monitor applications to ensure that a threat actor does not gain inappropriate access, and document all sessions just in case they do (insider threats) (Haber and Hibbert, 2018). PAM is about ensuring - and documenting - that only people with the proper authorization can administer critical systems.

A technology evaluation require a baseline to help organization choosing the right solution. This paper examines the role of Privileged Access Management (PAM) in executing the controls specified by the standard and highlights how the use of a seamless PAM solution meets some key ISO 27001 recommendations while decreasing the cost to meet others. Each section on ISO 27001 will analyze and map their respective controls with PAM solution, to meet and facilitate compliance with the standard. Our main contribution on this work is a matrix compliance of ISO 27001 Annex Control related to PAM solution, to enable end user reviewing PAM technology based on ISO 27001 control.

2. Information Security Management System (ISMS)

2.1. ISO 27001:2013

ISO 27001 is the latest incarnation of the original British Standard 7799, which was first published in 1995. It establishes a framework for an ISMS through policies and procedures spanning physical, technical, and legal controls. The controls framework is intended to help an organization accomplish the risk management goals through a meticulous and extensive compliance process. The ISO 27001 documentation describes the standard by saying it was created, "[to] provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISO/IEC 27001:2013, 2013). The standard is broadly embraced by IT professionals. The need for robust security is the most compelling driver of ISO 27001 adoption. According to a survey in the ISO 27001 Global Report 2015, almost 70% of respondents said that improving information security was the biggest driver for implementing ISO 27001 (*ISO 27001 Global Report 2015*, 2015). Technology neutral and top-down in approach, ISO 27001 suggests a six-stage planning process. The process includes defining a security policy, scoping the ISMS, doing a risk assessment, managing identified risks and selecting control objects and specific controls.

ISO 27001:2013 Annex Control contains 18 domains, of which the first 4 are introductions. The remaining 14 chapters cover the topics on Table 1. Table A.1 on Appendix A listed complete ISO 27001:2013 Annex Control.

Table 1 ISO 27001:2013 Annex Control Domain (ISO/IEC 27001:2013, 2013)

A.5. Information Security Policies	A.13. Communication security
A.6. Organization of Information Security	A.14. System acquisition, development and maintenance
A.7. Human Resource Security	A.15. Supplier relationships
A.8. Asset Management	A.16. Information security incident management
A.9. Access Control	A.17. Information security aspects of business continuity management
A.10. Cryptography	A.18. Compliance
A.11. Physical and environmental security	
A.12. Operation Security	

The standard, which consists of extensive documentation backed up by certification consultancies and audit processes, is intended to span multiple segments of an organization. While ISO 27001 does not

mandate any particular control, it does offer a controls checklist. These are listed in a related standard, ISO/IEC 27002:2013 (ISO/IEC 27001:2013, 2013). Other related standards offer implementation guidance (ISO 27003), metrics (ISO 27004) and auditing guidelines (ISO 27007) (*ISO 27000 Family of Standards*, 2018). For the purposes of simplicity, this paper considers this collection of related standards to effectively comprise ISO 27001.

2.2. Privileged Access Management (PAM)

PAM refers to the solutions and processes that enable IT departments to manage and audit the activities of all "privileged users" (Haber and Hibbert, 2018). A privileged user has administrative access to critical systems and data. For instance, a person who is authorized to set up and delete email accounts on Microsoft Exchange Server is a privileged user. Like any privilege, "root" privileges should only be extended to trusted people (Harley and Lee, 2006). Privileges should also be revoked when the need expires.

PAM keeps an organization safe from accidental or deliberate misuse of privileged access (Haber and Hibbert, 2018). For this reason, PAM should figure prominently into the implementation of ISO 27001. An ISMS needs to keep track of employees and contractors as well as remote or even automated users. Some privileged users can even override existing security protocols. If administrators can make unauthorized system changes, access forbidden data and then hide their actions that exposes the organization to serious risk. In ISO 27001 terms, a privileged user might be able to undermine much of the ISMS, either accidently or deliberately.

2.3. Privileged Access Management Component

Privileged Access Management (PAM) provides an automated password and session management solution that provides secure access control, auditing, alerting, and recording for any privileged account. The technology is designed to manage a local or domain shared administrator account; a user's personal admin account; service, operating system, network device, database (A2DB), and application (A2A) accounts; and even SSH keys, cloud, and social media (Haber and Hibbert, 2018). PAM enables the effective implementation of ISO 27001 by offering a secure, streamlined way to authorize and monitor all privileged users for all relevant systems. Particularly, it (Carson, 2017) :

- Grants privileges to users only for systems on which they are authorized.
- Grants access only when it's needed and revokes access when the need expires.
- Avoids the need for privileged users to have or need local/direct passwords.
- Centrally and quickly manages access over a disparate set of heterogeneous systems.
- Creates an unalterable audit trail for any privileged operation.

Gartner define two distinct tool categories have evolved as the predominant focus for security and risk management leaders considering investment in PAM tools (Felix Gaehtgens, Anmol Singh and Dale Gardner, 2017):

- **Privileged account and session management (PASM)**: Privileged accounts are protected by vaulting their credentials. Access to those accounts is then brokered for human users, services and applications. Sessions are established with possible credential injection, and full session recording. Passwords and other credentials for privileged accounts are actively managed (i.e., changed at definable intervals or upon occurrence of specific events).
- **Privilege elevation and delegation management (PEDM)**: Specific privileges are granted on the managed system by host-based agents to logged in users. This includes host-based command control (filtering), and also privilege elevation, the latter in the form of allowing particular commands to be run with a higher level of privileges.

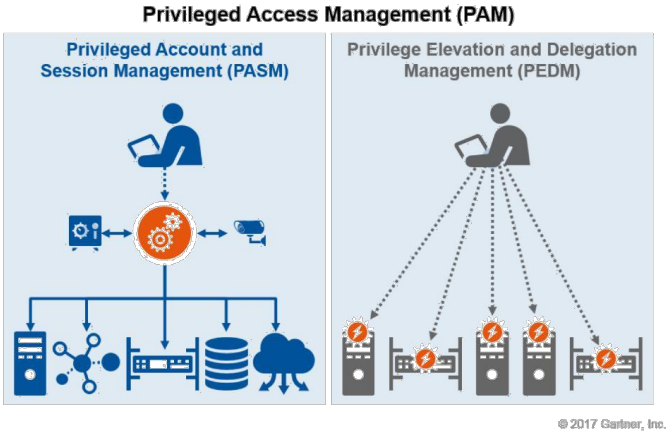

Figure 1 Privileged Access Management Tools (Felix Gaehtgens, Anmol Singh and Dale Gardner, 2017)

Privileged Access Management solutions vary architecturally. However, most offer the following components working together.

2.3.1. Access Management

Governs access to privileged accounts and creates a single-entry point, responding to ISO 27001 access control policy definition and policy enforcement. The privileged user requests access to a system through the Access Manager. The Access Manager is aware of which systems the user can access and his or her specified level of privilege. A super admin can add/modify/delete privileged user accounts on the Access Manager, thus reducing the risk that a former employee will retain access to a critical system. It also provides super admins with a centralized view of all session history held by privileged users, restoring complete visibility and control over strategic equipment (Haber and Hibbert, 2018).

2.3.2. Password Management

Password Management is a simple security function that helps a user store and organize passwords. Prevents privileged users from knowing the actual passwords/credentials to critical systems (Haber and Hibbert, 2018). A password vault can also preclude manual overrides on physical devices, a risk addressed by the physical controls described in ISO 27001 Section A.11. In this case, the PAM system stores passwords in a secure vault and opens access to a system for the privileged user once he or she has been approved for access. It can also extends administrator's password management policies by enforcing credential protection mechanisms such as A2A PM (Application-to-Application-Password-Management), automatic password rotation, and so on.

2.3.3. Session Management

Tracks privileged user connections and activities on target systems. A Session Management module provides real-time monitoring and record of all user activities to prevent incidents and conduct postmortem analyses and audits (Haber and Hibbert, 2018). PAM will help organization to adopt four eyes principle to have one of mutual accountability. Each individual is accountable to another, removing the risk of completely autonomous decisions, and increasing the likelihood that errors will be detected.

CA Technologies (*CA Inc. Common Stock (CA)*, 2018), leader in PAM market released PAM Buyer Guide to provide feature check list when planning to invest PAM Solution. Combining Gartner PAM Market Guide (Felix Gaehtgens, Anmol Singh and Dale Gardner, 2017) with CA PAM Buyer Guide ('Buyer's Guide: Privileged Access Management', 2016), PAM Domain solution matrix shown on Table B.1 on Appendix B.

3. Mapping ISO 27001:2013 Annex Controls to PAM Feature Domain

As discussed on Section 2, ISO 27001:2013 contains of 14 Annex Controls, PAM feature domain also defined by combining Gartner market Guide and CA PAM Buyers Guide. To map the ISO 27001:2013 standard into the PAM Feature Domain, it is necessary to define the method in order not to miss any security requirement. The steps to mapping the ISO 27001:2013 Annex to PAM will be following these below diagram.

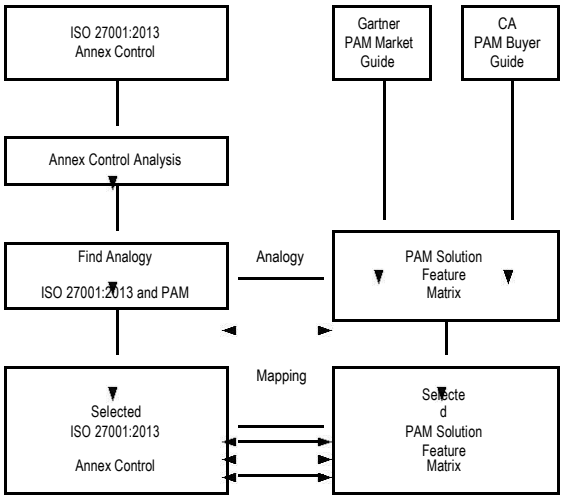

Figure 2 Mapping ISO 27001:2013 and PAM Solution

3.1. ISO27001:2013 Annex Control Analysis

The first steps, it is necessary to analyse and identify the structure of the ISO 27001:2013 Annex Control. The control contain of 14 domain (A.5-A.18). Mapping methods will be focusing on this domain and control.

3.2 Find analogy between both documents

The second steps, to find the analogy between Annex and PAM feature. Each control can be directly extracted from the PAM domain feature. Several of the controls contained in the ISO 27001:2013 standard discuss access control and PAM directly, even if the specification does not refer to PAM by name. In general, the principles of PAM underscore the entire spectrum of access controls in ISO 27001.

3.3 Mapping Annex Control to PAM Domain

The final steps, mapping the annex control to PAM domain feature. The structure of mapping table will contains the complying matrix of Annex and PAM feature related to the control.

4. Complying Matrix ISO 27001:2013 and PAM Feature Domain

4.1. Annex (A.6) Organization of Information Security

PAM helps companies respond to some of the controls highlighted in the section A.6 of ISO 27001:2013. Particularly, it answers the controls A.6.1.1 information security roles and responsibilities which lays ground for the definition and allocation of user or authority roles, as well as A.6.1.2 Segregation of duties. PAM provides administrators with the means to create, adjust, or delete fine-grained groups of users and sub-users [PAM.1.1]. It helps administrators have high visibility over the number of users within their system and allocate roles in a fluid manner [PAM.1.2]. At the same time, administrators can directly assign users the right level of privilege from a central point of command, thereby allowing them

respond to the principle of least privilege and segregate duties appropriately [PAM.1.2]. With each role and privilege clearly defined, PAM mitigates the risk of unauthorized or negligent activity within organizations' core network [PAM.1.6].

4.2. Annex (A.9) Access Controls

Annex A.9 in particular, which provides access controls, discusses PAM both directly and indirectly. The control specified in A.9.2.3 Management of Privileged Access Rights, reads, "The allocation and use of privileged access rights shall be restricted and controlled." A.9.4.4 Use of Privileged Utility Programs, has a control which specifies, "The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled." PAM can play in the execution of ISO 27001 Access Controls. For example, A.9.2.2 User Access Provisioning, offers a control where access rights can be assigned or revoked [PAM.1.1 PAM.1.2]. A The PAM solution can also terminate privileged access rights upon employee termination, as specified in A.9.2.6 Removal or Adjustment of Access Rights [PAM1.6].

4.3. Annex (A.11) Physical and Environmental Security

Physical and environment security might seem far from system access management issues. However, the two topics are closely linked. Control A.11.1 Secure Areas, has the objective, "To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities." Physical access can easily translate into data and systemic access. Unauthorized physical access to a system exposes an organization to the risk of improper administrative actions, such as deleting accounts or reconfiguring security settings. A PAM solution with a password vault lets privileged users do whatever they need to do without requiring any physical access to the hardware itself [PAM1.4]. In many traditional IT environments, admins had to manually reset servers, so physical access was expected. The practice created risk, though, which PAM mitigates [PAM.1.4 PAM.1.7].

4.4. Annex (A.15) Supplier Relationships

In many modern enterprises, supplier personnel may need privileged system access. Outsourced IT vendors, some of whom might be on different continents, may need to have "root" access to critical systems. Control A.15.1 Information Security in Supplier Relationships, acknowledges this reality. The control objective for A.15.1 is, "To ensure protection of the organization's assets that is accessible by suppliers." To protect an organization's IT assets from unauthorized access by suppliers, the PAM solution can define and enforce agreed-upon access policies [PAM.1.4]. The PAM solution should also provide auditability that enables both supplier and client to verify that the policies are being followed [PAM.3.1, PAM.3.3]. Controls A.15.1.1. and A.15.1.2 both address the requirement for establishing security policies in supplier relationships and agreements. PAM makes it possible to be specific about policies and prove compliance. PAM solutions that provide session management enable administrators to be aware of what happens on their systems, including through remote access [PAM.3.7]. Session management creates and audit trail and a high level of traceability of activities done on privileged accounts [PAM.3.7]. By being able to monitor suppliers with privileged account access, the PAM solution bolsters compliance with ISO 27001 control A.15

4.5. Annex (A.5) Management direction for information security

Even when a security policy is not directly related to PAM, PAM may well be a part of the policy, because privileged access underpins many other security policies. If an organization unable control privileged access, then few of other policies will be effective. For example, a company may have an acceptable use policy for web browsers and email systems. However, if an admin can delete accounts and erase browsing histories without anyone knowing, that will make the control deficient [PAM.1.1].

4.6 Annex (A.12) Operations Security

PAM also plays a role in operations security. Enriched by a Session Manager component, a PAM solution should be able to record and track all privileged user session activities at all times, thereby contributing to a secured operations flow on critical resources [PAM.3.1 PAM.3.5].

4.7 Annex (A.16) Information Security Incident Management

PAM figures into information security incident management, which is addressed by control A.16. For example, control A.16.1 Management of Information Security Incidents and Improvements, aims, "To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses." A PAM solution that can provide security managers with accurate information about privileged account sessions thanks to high traceability and monitoring capacities [PAM.3.1 PAM.3.3 PAM.3.5]. A PAM solution also able to provide instant reporting on any administrative sessions that took place on targeted systems can give security managers a working narrative of the incident [PAM.1.7].

4.8 Annex (A.18) Compliance with Internal Requirements

The controls specified in A.18 cover compliance with internal requirements. These requirements may be driven by internal policy as well as by legal and contractual requirements (A.18.1) or regulatory schemes (A.18.1.1). The objective of A.18.1 is "To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements." PAM can play an important role in ensuring this sort of compliance [PAM.2.5 PAM.3.7]. Privileged access management may be directly required by compliance programs. Compliance usually requires documentation. PAM enables the organization to document how it defines and enforces privileged access controls. PAM also provides logs of privileged sessions for use in compliance audits [PAM.3.3].

5. CONCLUSION

PAM solution facilitates ISO 27001 compliance by creating an access gateway for system admins that uses single sign-on (SSO). This capability enables the IT department to define and enforce access policies for admins and other employees who need privileged access. PAM lets admins manage access rights and passwords to servers and other devices through a single console. Equally, Session Manager module offers super administrators seamless visibility over their information system, from the identity of the privileged users operating on it or authorized to do so, to a full disclosure of their activity in real time or after their session has closed. This setup lets the IT department adapt access privileges quickly in response to organizational change. IT department turnover also becomes less of an issue with this level of control, ensuring that critical servers cannot be accessed by individuals no longer authorized to do so. With all the work involved in ISO 27001 compliance, the PAM solution should offers a streamlined, low-overhead solution to the privileged access controls of the standard.

6. APPENDICES

6.1. Appendix A

Table A. 1 ISO 27001:2013 Annex Control (ISO/IEC 27001:2013, 2013)

Domain	Control Objective	Controls	
A.5 Information Security Policies	A.5.1 Management direction for information security	A.5.1.1	Policies for information security
		A.5.1.2	Review of the policies for information security
A.6 Organization of information security	A.6.1 Internal organization	A.6.1.1	Information security roles and responsibilities
		A.6.1.2	Segregation of duties
		A.6.1.3	Contact with authorities
		A.6.1.4	Contact with special interest groups
		A.6.1.5	Information security in project management
	A.6.2 Mobile devices and teleworking	A.6.2.1	Mobile device policy
		A.6.2.2	Teleworking
A.7 Human resource security	A.7.1 Prior to employment	A.7.1.1	Screening
		A.7.1.2	Terms and conditions of employment
	A.7.2 During employment	A.7.2.1	Management responsibilities
		A.7.2.2	Information security awareness, education and training
		A.7.2.3	Disciplinary process
	A.7.3 Termination and change of employment	A.7.3.1	Termination or change employment responsibilities
A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.1	Inventory of assets
		A.8.1.2	Ownership of assets
		A.8.1.3	Acceptable use of assets
		A.8.1.4	Return of assets
	A.8.2 Information classification	A.8.2.1	Classification of information
		A.8.2.2	Labelling of information
		A.8.2.3	Handling of assets
	A.8.3 Media handling	A.8.3.1	Management of removable media
		A.8.3.2	Disposal of media
		A.8.3.3	Physical media transfer
A.9 Access control	A.9.1 Business requirements of access control	A.9.1.1	Access control policy
		A.9.1.2	Access to networks and network services
	A.9.2 User access management	A.9.2.1	User registration and de-registration
		A.9.2.2	User access provisioning
		A.9.2.3	Management of privileged access rights
		A.9.2.4	Management of secret authentication information users
		A.9.2.5	Review of user access rights
		A.9.2.6	Removal or adjustment of access rights
	A.9.3 User responsibilities	A.9.3.1	Use of secret information
	A.9.4 System and application access control	A.9.4.1	Information access restriction
		A.9.4.2	Secure log-on procedures
		A.9.4.3	Password management systems
		A.9.4.4	Use of privileged utility programs
		A.9.4.5	Access control to program source code
		A.9.4.5	Access control to program source code
A.10 Cryptography	A.10.1 Cryptographic controls	A.10.1.1	Policy on the use of cryptographic controls
		A.10.1.2	Key management
	A.11.1 Secure areas	A.11.1.1	Physical security perimeter

		A.11.1.2	Physical entry controls
		A.11.1.3	Securing offices, rooms and facilities
		A.11.1.4	Protecting against external and environmental threats
		A.11.1.5	Working in secure areas
		A.11.1.6	Delivery and loading areas
A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.1	Equipment siting and protection
		A.11.2.2	Supporting utilities
		A.11.2.3	Cabling security
		A.11.2.4	Equipment maintenance
		A.11.2.5	Removal of assets
		A.11.2.6	Security of equipment and assets offpremises
		A.11.2.7	Secure disposal or reuse of equipment
		A.11.2.8	Unattended user equipment
		A.11.2.9	Clear desk and clear screen policy
A.12 Operation Security	A.12.1 Operational procedures and responsibilities	A.12.1.1	Documented operating procedures
		A.12.1.2	Change management
		A.12.1.3	Capacity management
		A.12.1.4	Separation of development, testing and operational environments
	A.12.2 Protection from malware	A.12.2.1	Controls against malware
	A.12.3 Backup	A.12.3.1	Information backup
	A.12.4 Logging and monitoring	A.12.4.1	Event logging
		A.12.4.2	Protection of log information
		A.12.4.3	Administrator and operator logs
		A.12.4.4	Clock synchronization
	A.12.5 Control of operational software	A.12.5.1	Installation of software on operational systems
	A.12.6 Technical vulnerability management	A.12.6.1	Management of technical vulnerabilities
		A.12.6.2	Restrictions on software installation
	A.12.7 Information systems audit considerations	A.12.7.1	Information systems audit controls
A.13 Communications security	A.13.1 Network security management	A.13.1.1	Network controls
		A.13.1.2	Security of network services
		A.13.1.3	Segregation in networks
	A.13.2 Information transfer	A.13.2.1	Information transfer policies and procedures
		A.13.2.2	Agreements on information transfer
		A.13.2.3	Electronic messaging
		A.13.2.4	Confidentiality or non-disclosure agreements
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	A.14.1.1	Information security requirements analysis and specification
		A.14.1.2	Securing application services on public networks
		A.14.1.3	Protecting application services transactions
	A.14.2 Security in development and support processes	A.14.2.1	Secure development policy
		A.14.2.2	System change control procedures
		A.14.2.3	Technical review of applications after operating platform changes
		A.14.2.4	Restrictions on changes to software packages
		A.14.2.5	Secure systems engineering principles
		A.14.2.6	Secure developments environments
		A.14.2.7	Outsourced developments
		A.14.2.8	System security testing
		A.14.2.9	System acceptance testing
	A.14.3 Test data	A.14.3.1	Protection of test data
		A.15.1.1	Information security policy for suppliers relationships

A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.2	Addressing security within supplier agreements
		A.15.1.3	Information and communication technology supply chain
	A.15.2 Supplier service delivery management	A.15.2.1	Monitoring and review of supplier services
		A.15.2.2	Managing changes to supplier
A.16 Information management security incident	A.16.1 Management of information security incidents and improvements	A.16.1.1	Responsibilities and procedures
		A.16.1.2	Reporting information security events
		A.16.1.3	Reporting information security weaknesses
		A.16.1.4	Assessment of and decisions on information security events
		A.16.1.5	Response to information security incidents
		A.16.1.6	Learning from information security incidents
		A.16.1.7	Collection of evidence
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1	Planning information security continuity
		A.17.1.2	Implementing information security continuity
		A.17.1.3	Verify, review and evaluate information security continuity
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.1	Identification of applicable legislation and contractual requirements
		A.18.1.2	Intellectual property rights
		A.18.1.3	Protection of records
		A.18.1.4	Privacy and protection of personally identifiable information
		A.18.1.5	Regulation of cryptographic controls
	A.18.2 Information security reviews	A.18.2.1	Independent review of information security

6.2. Appendix B

Table B. 1PAM Domain feature mapping ('Buyer's Guide: Privileged Access Management', 2016; Felix Gaehtgens, Anmol Singh and Dale Gardner, 2017)

Domain	Control	
PAM.1 Access Management	PAM.1.1	PAM.1.1 Control access to privileged accounts, including shared and "firecall" (emergency access) accounts.
	PAM.1.2	Delegate, control and filter privileged operations that an administrator can execute.
	PAM.1.3	Require high-trust authentication for privileged access by either providing or integrating with other multifactor solutions to ensure required levels of trust and accountability.
	PAM.1.4	Implement workflow features for administrative users to request access, and for authorized approvers to grant this access.
	PAM.1.5	Access to shared accounts can be contingent on additional workflow approvals and/or high-trust MFA. An audit trail documents all privileged account use.
	PAM.1.6	Provides a zero-trust model where all access is denied, unless it is specifically permitted
	PAM.1.7	Providing full attribution for user activities using shared passwords
	PAM.1.8	Supports a broad set of end-point types like UNIX®/Linux® via SSH or Telnet, Microsoft, Windows® and published apps via RDP, databases, mainframe systems via TN3270 or TN5250, and network devices via SSH or Telnet
	PAM.1.9	Supports local application execution, invoking local/desktop application connections to managed devices
PAM.2 Password Management	PAM.2.1	Automatically randomize, manage and vault passwords and other credentials for administrative, service and application accounts.
	PAM.2.2	Eliminate hard-coded passwords by making them available on demand to applications.
	PAM.2.3	Provide single sign-on (SSO) for privileged commands and actions in a secure manner, such that credentials are not revealed.
	PAM.2.4	Support "break the glass" scenarios for emergency and disaster recovery purposes, including the support for firecall accounts.
	PAM.2.5	Users of privileged accounts should not be allowed to see or access the actual passwords for these accounts, passwords for shared accounts must not be shared, which can lead to uncontrolled access.
	PAM.2.6	Rotating credentials and changing them in situ — that is, in the place where they are held by the system, application or service. Examples are Windows services that run under local or domain service accounts, whenever the password is changed, the services require that their service configuration is updated on each local system where the services run.
	PAM.2.7	Automatic generation of credentials for continuous deployment/continuous integration and orchestration tools, as new instances are built, such as in elastic scalable environments.

	PAM.2.8	Managing cryptographic access keys and other credentials used within containers, such as Docker.
	PAM.2.9	Allowing an application to retrieve the password from the vault through a network-protocol-based API.
	PAM.2.10	By use of application-to-application password management (AAPM) agents that are installed on local systems and allow applications to access credentials using host-based access control mechanisms, described in the next section.
	PAM.2.11	Application fingerprinting or checksum verification of the application, its configuration and other dependent files to prevent tampering.
	PAM.2.12	Environment verification, such as the user ID or process under which the application is started, from which directory it is started, and so on.
	PAM.2.13	One-time password mechanisms, where after every invocation the next sequence password is generated from a seed, stored and verified upon subsequent invocation.
	PAM.2.14	Automates the creation, use and change of passwords, SSH session keys and other credentials
	PAM.2.15	Centralizes the administration, storage, release and audit of credentials
	PAM.2.16	Store credentials in an encrypted safe, protecting them using managed keys generated, stored, and used via software or FIPS-140-2 validated HSM
	PAM.2.17	Scales by managing high volume credentials (across multi-site, hybrid enterprise environments)
	PAM.2.18	Provides built-in replication of the credential safe/password vault, aiding disaster recovery
	PAM.2.19	Manages and modify credentials based on flexible password change policies including rotating passwords at scheduled intervals
	PAM.2.20	Provides automated login to managed endpoints using privileged credentials without revealing the credentials to users
	PAM.2.21	Provides transparent login for secondary credentials such as SUDO, databases, and other targets that require secondary authentications
	PAM.2.22	Provides learn mode for RDP applications and web applications, simplifying credentials acquisition when using RDP published applications and web-based applications
	PAM.2.23	Offers support for dual credential approval, requiring approvals by designated users prior to allowing access to credentials for managed accounts
	PAM.2.24	Provides detailed application-to-application password audits and activity reporting
	PAM.2.25	Allows specific security controls around requesting applications or scripts, including support for: Specific UIDs executing the script or application, The calling path, The file path, Checksum validation and denies the requesting application's access to the credential if any or all of the above return a false or untrue value
	PAM.2.26	Allows for the use of an encrypted cache to speed up transaction times and support outage situations
PAM.3 Session Management	PAM.3.1	Monitor, record and audit privileged access, commands and actions.
	PAM.3.2	Provides session recording and playback for privileged user sessions across RDP/VNC, SSH and cloud management consoles or web-based systems
	PAM.3.3	Generates comprehensive logs of all requests and responses by the system, including a complete, detailed account of what happened on sensitive systems and who performed a specific activity
	PAM.3.4	Provides full-resolution capture of privileged user sessions
	PAM.3.5	Provides DVR-like playback controls for session replay, allowing session review from beginning to end, back up and replay portions of a session, or fast-forwarding to specific points of interest, like jumping to specific points in the timeline to evaluate violations
	PAM.3.6	Provides comprehensive support for web application session recording, including high-fidelity session tracking for web-based applications and management interfaces (for example, AWS Management Console, VMware interfaces and the Microsoft Office 365 administrative portal)
	PAM.3.7	Supports always-on session recording and auto-start session recording when a policy violation is detected
	PAM.3.8	Provides extensive logging capabilities of the critical interactions that take place between hybrid clouds and individual users, supporting configuration management solutions like
	PAM.3.9	Puppet or Chef, and a broad range of application programs employing AWS software development kits
	PAM.3.10	Records and forwards session activity to SIEM tools for further examination and automation

REFERENCES

2018 Data Breach Investigations Report (2018). Verizon.

'Buyer's Guide: Privileged Access Management' (2016). CA Technologies.

CA Inc. Common Stock (CA) (2018) *NASDAQ.com*. Available at: https://www.nasdaq.com/symbol/ca (Accessed: 25 August 2018).

Carson, J. (2017) 'Privileged Account Management For Dummies®, Thycotic Special Edition', p. 29.

Felix Gaehtgens, Anmol Singh and Dale Gardner (2017) 'Market Guide for Privileged Access Management'. Gartner.

Haber, M. J. and Hibbert, B. (2018) *Privileged Attack Vectors*. Berkeley, CA: Apress. doi: 10.1007/978-1-4842-3048-0.

Harley, D. and Lee, A. (2006) 'The Root of All Evil? - Rootkits Revealed', p. 17.

ISO 27000 Family of Standards (2018) *The ISO/IEC 27000 Family of Information Security Standards*. Available at: https://www.itgovernance.co.uk/iso27000-family (Accessed: 24 August 2018).

ISO 27001 Global Report 2015 (2015). IT Governance.

ISO/IEC 27001:2013 (2013) 'ISO/IEC 27001:2013(E) Information technology-Security techniques-Information security management systems -Requirement'. ISO/IEC 2013.

Itradat, A. *et al.* (2014) 'Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study', *Financed by Scientific Research Support Fund*, 8(2), p. 102.

'Three Important Reasons for Privileged Identity Management' (2015). ENTERPRISE MANAGEMENT ASSOCIATES. Available at: https://www.infosecurityeurope.com/__novadocuments/376960?v=636372817068200000 (Accessed: 24 August 2018).