OSIRIUM WHITEPAPER

ISO27001 Compliance
Accelerating compliance with Privileged Access Security

OSIRIUM

Accelerating compliance with Privileged Access Security

Introduction

ISO 27001:2013 (and its recent minor update in 2017) are foundational standards for information security. ISO27001 is broad ranging but its core requirements help organisations to build, implement, and improve systems management security. Besides being best practice recommendations in their own right, they can also be used as the starting point for compliance with standards such as GDPR, PCI DSS, NIS and more.

ISO27002 is a supplemental standard to help implement an Information Management Security Management System (ISMS). ISO27002 delves into more details on how to achieve compliance. It also has a broad scope, with 14 separate security controls (or "clauses"), some of which are out of scope for this whitepaper.

This guide highlights key elements of ISO27001 and how privileged access security is a key capability to not only achieve ISO27001 certification but also to make on-going compliance a low-impact activity.

About Osirium

Osirium is the leading UK-based vendor of Privileged Access Security (PAS) solutions. Osirium's cloud and on-premise products protect critical shared IT infrastructure and endpoints, and securely streamline IT operations to deliver digital transformation fast.

Osirium's PAS solution includes modern **Privileged Access Management (PAM)** to protect valuable services and enables managed access by third-party vendors and partners. It includes high-availability clustered servers, session recording, just-in-time approvals and simple deployment.

PAS also includes **Osirium Automation**, powered by the secure, flexible Privileged Process Automation (PPA) framework, to automate privileged tasks for streamlined and secure IT operations. Secure automation allows tasks that normally need multiple IT experts to be delegated to first-line help desk engineers or users across the business.

It also includes **Privileged Endpoint Management (PEM)** to remove local administrator accounts and manage applications approved to run with elevated privileges. Removing local admin rights is a critical part of any "least privilege" policies.

The Key Elements of ISO27002

In this section, the key requirements of selected clauses in ISO27002 are listed along with how Privileged Access Security can be used in that context.

6. Organization of information security

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

This clause covers a wide range of information security issues, for the context of this document, section 6.2.1 which covers mobile and teleworking is relevant.

6.2.2 Teleworking	
A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	**PAM is particularly relevant to manage remote access to IT systems with privileged accounts. PAM can control who has access to which systems, sessions can be monitored in realtime and recorded for later review. Access can be limited to specific time slots to reduce risk.**

8. Asset Management

Objective: To identify organizational assets and define appropriate protection responsibilities.

This section covers all types of asset, not just physical devices but also the data held on the organization's systems.

8.1.2 Ownership of Assets	
The asset owner should … b) ensure that assets are appropriately classified and protected; … d) ensure proper handling when the asset is deleted or destroyed.	**Admin accounts should be owned by PAM, ensuring the credentials such as passwords confirm to the corporate standards, are never exposed to users, can easily be rotated or removed when the asset is deleted or destroyed.**
In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.	**Osirium PAM can group devices and users within groups to allow policies and access at the group level rather than individual. It also makes asset inventory and audit easier.**

9. Organization of information security

Objective: To limit access to information and information processing facilities.

Access control policies are key to most other security management requirements. In particular, administrator or other privileged accounts need to be well managed as they are the keys to managing all other systems, access and users. Access control policies also need to consider regular re-certification or auditing and update or removal when access is no longer needed.

The Key Elements of ISO27002 - Continued

9. Organization of information security

9.1.2 Access to networks & network devices	
Users should only be provided with access to the network and network services that they have been specifically authorized to use.	Osirium PAM focuses on Access control of Privileged Users and Accounts to separate people from passwords. PAM provides an operational model through separation of Identity In, Role Out based on least privilege. Profiles map the identity of a user to the role that they should have on a system, device or application.
9.2.1 User registration and deregistration	
A formal user registration and deregistration process should be implemented to enable assignment of access rights	Osirium PAM manages the entire lifecycle of privilege account access which is independently mapped to a user/s. Accounts can easily have their state level increased or reduced. This enables each device to have its accounts managed in the way that best suits the security policy.
9.2.2 Management of privileged access rights	
The allocation and use of privileged access rights should be restricted and controlled	The management of privileged access rights is core functionality for Osirium PAM. It is used for full control of all privilege accounts and all system access. Osirium allows device access to be granted at a very granular level and to assign specific roles to individuals or groups of individuals. Because the accounts have been created personalised to each user, they can be aligned to a particular set of rights or permissions on the end device, therefore no more sharing the highest-level account.
9.2.4 Management of secret authentication information of users	
The allocation of secret authentication information should be controlled through a formal management process.	Osirium PAM helps enforce a secret authentication process as we inject credentials to the server, device or application during the user connection. We would deem usernames and passwords to be secret authentication information for users. PAM uses long, complex, randomly created passwords, making dictionary and brute force attacks futile. Password rules can be set per device to ensure any password policies on devices are met. Different passwords are used for every account on every device managed by Osirium.

The Key Elements of ISO27002 - Continued

9. Organization of information security

9.2.5 Review of user access rights	
Asset owners should review users' access rights at regular intervals.	Osirium can help review privilege users' access rights at three regular intervals; • Analytics to show what users have used (Past) • Real time dashboard (Present) • Access analysis reports (Future) PAM Password Lifecycle Management enables asset owners to audit user access rights on a regular basis. Automation allows account or group access rights to be delegated to asset owners or managers to review and update access as needed without complex spreadsheet or paper processes which are liable to human-error and highly time-consuming.
9.2.6 Removal or adjustment of access rights	
The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Osirium PAM can be used to both remove or adjust privilege access rights of all employees and external party users. PAM and Automation can automate standard system administration workflow to enforce business process and policy. As an example, an automated playbook to remove access rights and credentials as part of an employee termination process.
9.3.1 Use of secret authentication information	
Users should be required to follow the organization's practices in the use of secret authentication information.	Osirium PAM can enforce secret authentication information policy to all privilege accounts including personalised, shared and generic accounts. Generic Account Access allows 3rd party access to infrastructure devices/systems using generic Admin/Administrator accounts WITHOUT revealing the password. Intermediate levels of accounts such as read-only can also be shared. Personalised Account Access Create and fully manage the lifecycle of personalised accounts for each 3rd party requiring access, including the automatic renewal of long and strong passwords, without revealing them to the SysAdmin teams. 3rd parties are automatically granted secure access using their own credentials, with full audit trails recorded on both the end devices and Osirium too.

The Key Elements of ISO27002 - Continued

9. Organization of information security

9.4.1 Information and access restrictions	
Access to information and application system functions should be restricted in accordance with the access control policy.	Osirium can help enforce and audit all privileged user access to critical systems and information of a privileged layer in accordance with the access control policy.
9.4.2 Secure log-on procedures	
Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	Osirium helps organisations to implement strong access controls of privilege users and privilege accounts to all systems and applications. Access to Osirium can be tied into two factor authentication (2FA) services via radius and Single Sign On (SSO) is used when connecting to devices. Strong Authentication Support: SysAdmins can log into Osirium using their existing standard account username and password. Alternatively, two factor or token-based authentication via RADIUS is available for stronger authentication options. SSO with Password Injection Security: Single Sign On is performed by injecting the required credentials as the connection request passes through Osirium's proxies. This means passwords are never sent down to the client, thereby removing the possibility that sniffing memory, or looking at command strings within the process tree, will ever reveal a password .
9.4.3 Password Management System	
Password management systems should be interactive and should ensure quality passwords.	Osirium enables strong long, complex, quality passwords and single sign on (SSO) mechanisms allowing a strengthened password management system for privileged users.
9.4.4 Use of privileged utility programs	
The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	Osirium PAM helps apply least privilege and controls the use of and access to utility programs at privilege layer and tightly control and audit all connections.

The Key Elements of ISO27002 - Continued

10. Cryptography

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Cryptography covers both encryption of data and keys to access that data or the organization’s systems.

10.1.1 Policy on the use of cryptographic controls	
A policy on the use of cryptographic controls for protection of information should be developed and implemented.	**Osirium PAM can help automate and enforce cryptographic control policies via tasks run by privileged users.**
10.1.2 Key management	
A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	**Automation can be used for automated playbooks to create, manage and securely deploy keys.**

11. Equipment

Objective: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.

Managing the equipment lifecycle should include management of access to the equipment from acquisition to disposal.

11.2.7 Secure disposal or re-use of equipment	
All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	**Osirium PAM can help remove risks associated with disposing equipment containing storage media that may hold configuration data by removing any secret authentication information, which could open backdoors to client systems and networks to gain access to the organisation.**

12. Operations security

Objective: To ensure correct and secure operations of information processing facilities.

Operational procedures are intended to protect data and systems while being used by authorised users. To that end procedures should be well documented and understood by users. The best protection comes when processes are automated to prevent manual error or divergence from the documented process.

The Key Elements of ISO27002 - Continued

12. Operations security

12.1.1 Documented operating procedures	
Operating procedures should be documented and made available to all users who need them.	Osirium Automation uses "playbook" to automate corporate processes. The playbooks, written in low-code YAML, are the most accurate form of documentation as they define the actual steps that will always be executed. The Automation audit trail is used to prove that compliance in audits.
12.1.3 Change Management	
Changes to the organization, business procedures, information processing facilities and systems that affect information security should be controlled.	Osirium's Automation playbooks are versioned with a change history and only deployed into production use by authorised users.
12.1.14 Separation of development, testing and operational environments	
Development, testing and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.	Osirium Automation can be integrated with service desk management systems such as ServiceNow to have round-trip control and audit. For example, a change request may be reviewed and approved in Sevicenow which automatically invokes an Automation playbook which, in turn updates the Servicenow change request with the full audit trail. Change Management / History: Osirium's Session Recorder can act as an irrefutable change control record of what changes actually occurred in the infrastructure. As opposed to what the SysAdmin thought might have happened during their time on a device. Faster Error Remediation: Recordings can provide valuable insights as to why and when there was a misconfiguration of a device. It allows changes to be investigated and provides faster error remediation back to a stable and working environment.
12.2.1 Controls against malware	
Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Osirium PAM restricts the effectiveness of malware by removing the presence of privileged accounts from all admin workstations. Even if a device gets infected with malware they cannot escalate privilege which breaks an attackers kill chain. Osirium PEM allows local admin accounts to be removed from end user workstations. While approved applications can be run with elevated permissions, they can't install new software that has not been approved or does not match the approved version's fingerprint thus preventing installation of the malware in the first place. PAM and PEM can be used as part of a malware protection strategy: 'reduce your attack surface'.

The Key Elements of ISO27002 - Continued

12. Operations security

12.3.1 Information backup	
Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	PAM should be used to protect access to backup management systems. If those systems are compromised, then backup data is at risk. Osirium Automation tasks can be used to backup systems which may be outside the core corporate backup strategy. For example, backing up the configuration of devices which fall outside the normal scope of a traditional network backup solution is a valuable contributor to business continuity.
12.4.1 Event logging	
Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Osirium PAM sends rich logging information for both its own configuration changes and for connections and or tasks that flow through our virtual appliance which can then help enrich data in SIEM solutions. End to End Accountability: PAM provides an audit trail of who has accessed what, where, when, how and because the SysAdmin can be signed on with a personalised account. As a result, any audit trail created by the device itself will contain personalised login details, not just 'admin' did this, 'root' did that, which renders syslog information even more valuable to an SIEM solution. This can be done without any changes to the logging solution and no manual cross referencing.
12.4.3 Administrator and operator logs	
System administrator and system operator activities should be logged, these logs should also be protected and regularly reviewed.	Osirium PAM sends its own audit log via syslog. Audit logs from Automation tasks can also be centrally logged to the organization's SIEM systems.
12.4.4 Clock synchronization	
The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source.	Osirium tasks can be used to ensure all systems are configured and synchronised to use a single reference time source (ntp servers).

The Key Elements of ISO27002 - Continued

13. Communications security

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

Operational procedures are intended to protect data and systems while being used by authorised users. To that end procedures should be well documented and understood by users. The best protection comes when processes are automated to prevent manual error or divergence from the documented process.

13.1.1 Network controls	
Networks should be managed and controlled to protect information in systems and applications.	All IT Infrastructures are managed by Privileged Users, who are given elevated powers through accessing Privileged Accounts to ensure that the uptime, performance, resources, and security of the computers meet the needs of the business. It's the misuse of Privileged Accounts in the Hybrid-Cloud world which has become one of the most critical security challenges, because uncontrolled access to Privileged Accounts opens a "barn door" through which untrusted 3rd parties can compromise data and inflict cyber-attacks, ultimately causing irreparable damage to the business and its corporate reputation. Osirium creates a secure separation between the users system and credentials and the connection and credentials used for the system/device/application to be managed. Osirium ensures that device credentials never pass through the users system and therefore never risk interception. Osirium implements Enterprise Class Password Management to ensure that all the passwords it manages are the strongest possible for each of the device classes. It has full breakglass and roll-back features to cope with devices that leave the network or are restored from backups.
13.1.1 Network controls	
Groups of information services, users and information systems should be segregated on networks.	Osirium can help in enforcing network segregation through the control of privilege accounts
13.2.2 Agreements on information transfer	
Agreements should address the secure transfer of business information between the organization and external parties.	Osirium can control the flow of privileged information between the organisation and third parties particularly when providing system support (tech out). Device Techouts Collecting diagnostic technical information can be a tedious and time consuming task. A Tech-out task solves this by connecting to a device, running a recognized set of commands to collect diagnostic information and then copying it back to Osirium. Tech-outs can be stored for future examination and comparison with current issues.

The Key Elements of ISO27002 - Continued

13. Communications security

13.2.2 Agreements on information transfer - Continued	
Agreements should address the secure transfer of business information between the organization and external parties.	File Uploads: Files can be selected and uploaded TO devices as part of a task. e.g. this allows tasks to start with a file import and then other steps can be performed to check if the file had been processed correctly, for example through SQL commands. File Downloads: Files can also be downloaded FROM devices either during or at the end of a task. This would allow routine specific logs or reports to be downloaded to Osirium for diagnostic purposes, particularly if the SysAdmins did not have direct authorized privileged access to the device.

14. System acquisition, development and maintenance

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Security of information systems has to include the data within the systems are treated just as carefully as the physical devices, services and applications.

14.1.2 Securing application services on public networks	
Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification	From a Privileged account and access point of view, Osirium PAM can enforce strict security controls and provide strong security policy to public facing services be them privately hosted or hosted in the cloud.
14.2.2 System change control procedures	
Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.	Osirium can enforce change references needing to be recorded for all privilege access to all systems. Change Ticket Information: A free text input can be setup as a change ticket reference. Entering a valid format Change Ticket number prior to running the task will be logged in the audit trail of the task, allowing it to be searchable and found by ticket number search criteria.
14.2.7 Outsourced development	
Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification	Osirium PAM can audit, monitor and record all outsourced activity. Connection Alerts: Alerts can be raised whenever a 3rd party establishes a connection to a device or system. This provides realtime information on who is accessing and working on critical problems while they happen.

The Key Elements of ISO27002 - Continued

15. Supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

All organizations need to work with suppliers, outsourced services and partners who often need access to the organization's information systems. That access needs particular focus as there may be less control and more opportunities for attack from external partners.

15.1.2 Addressing security within supplier agreements	
All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	**Osirium PAM can manage and audit supplier connectivity – applying a least privilege model to secure the third-party access.** **Least Privileged Model:** **It is no longer necessary to issue the maximum level of access to everyone in the admin team.** **PAM applies a least-privilege security posture, ensuring that each privileged role, particularly those outsourced to 3rd party service providers, are given no more than the level of privileged necessary for them to fulfil their jobs.** **Time Windowed Access:** **3rd party access can be restricted to specific time windows, so whether overnight, at weekends or during routine daily maintenance, specific change windows can restrict write permissions to certain times. Read-only access control can be also used to complement the restricted write access, allowing for in-house diagnostics and troubleshooting.**
15.2.1 Monitoring and review of supplier services	
Organizations should regularly monitor, review and audit supplier service delivery.	**Osirium PAM allows monitoring and review of supplier services via Privileged Session Recording and privileged analytics.**

16. Information security incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

The response to a security incident is critical. The time to remediate the impact can make the difference to whether the organization can continue in business or not. Equally important is being able to learn what happened and use that learning to prevent future incidents.

16.1.7 Collection of evidence	
The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	**Osirium records privilege access to enable the review and audit of activity.** **Session Recording:** **All SysAdmin sessions passing through Osirium can be recorded. A visual capture allows a video style playback of each session (including a fast play mode) along with a thumbnail view to allow fast review of sessions.**

The Key Elements of ISO27002 - Continued

16. Information security incident management

16.1.7 Collection of evidence - Continued	
The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Session Shadowing: All SysAdmin sessions passing through Osirium can be viewed in real-time. This allows all admin activities, including 3rd party service providers, to be monitored as it happens. Keystroke Capture: As well as a visual recording of a session, all keystrokes are captured. Subsequently enabling the search and find facility to identify particular keystrokes during each session. Search by other Meta Information: The Device Access Report can search by a wide range of criteria. This includes date/time, user, device, access level, protocol and even the Window Titles as well.

Preparing for ISO27001

The first step to preparing for an ISO27001 assessment is to understand your current IT infrastructure and controls in place. Building the inventory of devices and accounts is largely a manual process. Osirium PAM can assist by discovering accounts defined within Active Directory and the accounts on those devices.

To assess the effectiveness of PAM, a free version of Osirium PAM is available (via **https://www.osirium.com/pam-express**). Once ready to consider a broader assessment, Osirium experts are available to discuss the options.

Osirium has been helping organisations achieve regulatory compliance, for many years. If you'd like to discuss best practices and options for simplifying your compliance audit, **please get in touch**.