ISO/IEC 27001 INFOSEC STANDARD

COMPLIANCE STANDARD

osirium.com

OSIRIUM

v2.0

OSIRIUM COMPLIANCE STANDARDS

OSIRIUM AND ISO/IEC 27001

International Organization for Standardization

TAKING THE COMPLEXITY OUT OF COMPLIANCE

How Osirium supports ISO 27001:2013 Access Control and System acquisition requirements. Created in partnership with Acuity Group.

OSIRIUM

SECURE • SCALE • SIMPLIFY

acuity GROUP
the specialists in
GRC MANAGEMENT SYSTEMS

OSIRIUM NEXT-GEN PRIVILEGED ACCESS MANAGEMENT (PXM): STATEMENT OF APPLICABILITY (SOA) FOR ISO27001:2013

Information Security Controls

Based on the analysis of the Information Assets, the appropriate IS Controls can be mapped and implemented to the appropriate assets, mitigating the impact of known and unknown threats, balancing the Physical, Logical and Information risk ratings.

Objective

To select and implement information security controls which provide appropriate and effective mitigation of inherited risks.

Background

Robust information security controls are required to minimise the potential for exploitation of known and perceived vulnerabilities within the businesses information assets.

Process

By reference to ISO 27002:2013, select appropriate and cost effective controls to address perceived risks to the businesses information assets. Implementation is to follow acknowledged industry best practice and be consistent across the Business.

Statement of Applicability

A documented 'Statement of Applicability' is to be created and maintained, listing the Information Security controls deemed by the company to be applicable under their ISO 27001:2013 certification scope together with brief details of how they have been implemented.

Software supplier: Statement of Applicability (SoA)

The table overleaf defines the Minimum Security Requirements (MSR) for the transmission and access of Client Services Information in relation to privileged users. Definitions of the required controls can be found in Appendix A.

Statement of Applicability

A defined table of applicable IS Control documents to maintain 'control' over the objectives of the Businesses Client Services Information needs, having considered the operational IS Risks (C.I.A. rated).

Software Supplier - Information Security Controls		Applicability
5.1	Management Direction for Information Security	N/A
6.1	Internal Organisation	N/A
6.2	Mobile Devices and Teleworking	N/A
7.1	Prior to Employment	N/A
7.2	During Employment	N/A
7.3	Termination and Change of Employment	N/A
8.1	Responsibility for Assets	N/A
8.2	Information Classification	N/A
8.3	Media Handling	N/A
9.1	**Business Requirements of Access Control**	**Applicable**
9.2	**User Access Management**	**Applicable**
9.3	**User Responsibility**	**Applicable**
9.4	**System and Application Access Control**	**Applicable**
10.1	**Cryptographic Controls**	**Applicable**
11.1	Secure Area	N/A
11.2	**Equipment**	**Applicable**
12.1	**Operational Procedures and Responsibilities**	**Applicable**
12.2	**Protection From Malware**	**Applicable**
12.3	**Backup**	**Applicable**
12.4	**Logging and Monitoring**	**Applicable**
12.5	Control of Operational Software	N/A
12.6	Technical Vulnerability Management	N/A
12.7	Information Systems Audit Considerations	N/A
13.1	**Network Security Management**	**Applicable**
13.2	**Information Transfer**	**Applicable**
14.1	**Security Requirements of Information Systems**	**Applicable**
14.2	**Security In Development and Support Processes**	**Applicable**
14.3	Test Data	N/A
15.1	**Information Security In Supplier Relationships**	**Applicable**
15.2	**Supplier Service Delivery Management**	**Applicable**
16.1	**Management of IS Incidents and Improvements**	**Applicable**
17.1	Information Security Continuity	N/A
17.2	Redundancies	N/A
18.1	Compliance With Legal and Contractual Requirements	N/A
18.2	Information Security Reviews	N/A

APPENDIX A - INFORMATION SECURITY CONTROLS

For detailed guides on 'how to' implement the Privileged User Security Controls below; ref: BS ISO/IEC 27002:2013 - Security techniques please contact Osirium.

A.9 ACCESS CONTROL

9.1 Business requirements of access control (A.9.1)

9.1.2	Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.

Osirium focuses on Access control of Privilege Users and Accounts to separate people from passwords. We provide an operational model through separation of **Identity In, Role Out** based on least privilege. By this we mean that we use profiles to map the identity of a user to the role that they should have on a system, device or application.

9.2 User access management (A.9.2)

9.2.1	User registration and deregistration	A formal user registration and deregistration process should be implemented to enable assignment of access rights.

Osirium manages the entire lifecycle of privilege account access which is independently mapped to a user/s.

Readily Change Account States
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	User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

Osirium can help automate the user access provisioning, making onboarding and offboarding efficient and cheaper to achieve the same goals. We can provision privilege users and then build tasks for provisioning standard users. Technically applying policy through automation.

9.2.3	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. We help provide full control of all privilege accounts and all system access.

Role Based Access Control
Osirium allows device access to be granted at a very granular level and to assign specific roles to individual 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's PxM Platform 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.

Complex Passwords
Osirium's PxM Platform 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.

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)

The PxM Platform's Password Lifecycle Management enables asset owners to audit user access rights on a regular basis.

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.

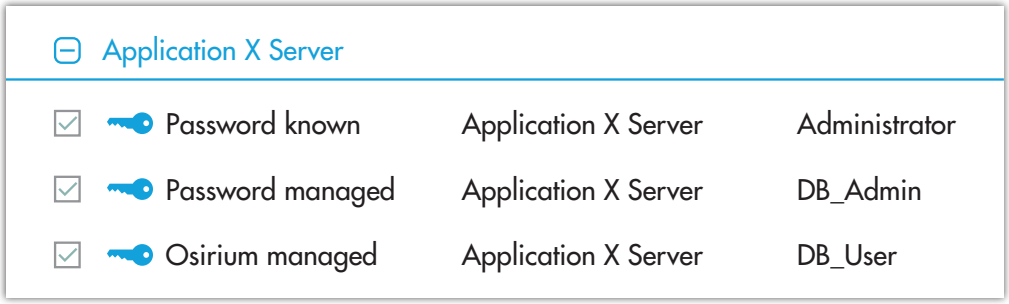
Osirium can be used to both remove or adjust privilege access rights of all employees and external party users. We have the ability to create tasks to help automate standard system administration workflow which can help enforce business process and policy. As an example we could offer tasks to aid the standard termination process or to help manage Third party access control.

9.3 User responsibilities (A.9.3)

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.

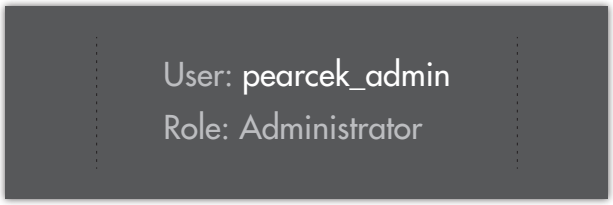
Osirium can enforce secret authentication information policy to all privilege accounts including personalised, shared and generic accounts.

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.



9.4 System and application access control (A.9.4)

9.4.1	Information and access restriction	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 helps apply least privilege and controls the use of and access to utility programs at privilege layer and tightly control and audit all connections.

A.10 CRYPTOGRAPHY

10.1 Cryptographic controls (A.10.1)

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 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.

Osirium's PxM Platform can help automate and enforce cryptographic key management policies via tasks run by privileged users.

Not standard functionality for the PxM Platform but we could help develop tasks to help with this process.

A.11 EQUIPMENT

11.2 Equipment (A.11.2)

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 could 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.

A.12 OPERATIONS SECURITY

12.1 Operational procedures and responsibilities (A.12.1)

12.1.3	Change management	Changes to the organization, business procedures, information processing facilities and systems that affect information security should be controlled.

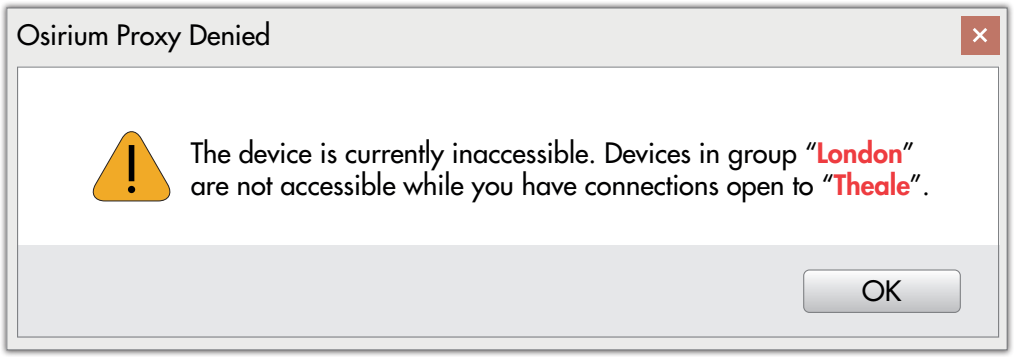
Osirium's PxM Platform's Task Automation could help manage and enforce the future capacity requirements in relation to privileged users within an organization.

12.1.4	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 tasks have a feature where we can link to and reference change tickets from ITSM solutions like ServiceNow so that any changes to the organisation , business processes and information process can be referenced in relation to privilege users.

Change Management / History
Osirium's Session Recorder can act as an irrefutable change control record of what changes actually occurred on 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 Protection from malware (A.12.2)

12.2.1	Controls against malware.	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Osirium restricts the effectiveness of malware by removing the presence of privilege accounts from all admin workstations. Even if a device gets infected with malware they cannot escalate privilege which means we can effectively break an attackers kill chain.

Osirium can be used as part of a malware protection strategy: 'reduce your attack surface'. You'll notice from the Killchain diagram that all attacks have to go through the escalate privileges stage. 99.9% of attacks do so by gaining access or control of Privileged Accounts. That's where Osirium helps. It separates people from passwords (PAM), and with it's task scheme (PTM) many people will never need access to a Privileged Account. Since the biggest attack vectors are the vulnerabilities of User's workstations and the phishability of the users themselves we'd say that Osirium was a major contribution to Cyber Safety.

12.3 Backup (A.12.3)

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.

Osirium tasks can be used to backup systems which may be outside the core corporate backup strategy. All devices covered by Osirium can be covered so we can effectively fill the gap and allow backup of configuration files of network devices and applications not managed via active directory or by COTS backup solutions.

Device Backups
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.

One does not require agents on the devices and actually invokes the vendors own commands to create a backup archive file which then gets copied and stored securely on the PxM Platform.

12.4 Logging and monitoring (A.12.4)

12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Osirium sends good 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
Osirium 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.

Timestamp	User Name	Transaction	Event
Wed Jan2 16:30:51 GMT 2016	nealt_admin	0-0	load config:
Wed Jan2 16:30:45 GMT 2016	walkers_admin	0-0	config load:
Wed Jan2 16:30:41 GMT 2016	walkers_admin	0-0	config save:
Wed Jan2 16:30:28 GMT 2016	parksz_admin	0-0	help:
Wed Jan2 16:29:41 GMT 2016	portere_admin	0-0	arp show:
Wed Jan2 16:29:30 GMT 2016	portere_admin	0-0	arp show:
Wed Jan2 16:29:21 GMT 2016	westa_admin	0-0	ssh(pam_audit): user=

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 sends its own audit log via syslog. We can also use tasks to ensure that other systems do the same. Osirium also sends connection and task logs via syslog giving SIEMs additional granular data to be able to report on privilege activity.

12.4.4	Clock synchronisation	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).

A.13 COMMUNICATIONS SECURITY

13.1 Network security management (A.13.1)

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 Privilege 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.

13.1.3	Segregation in networks	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 Information transfer (A.13.2)

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 privilege information between the organisation and third parties particularly when providing system support (tech out).

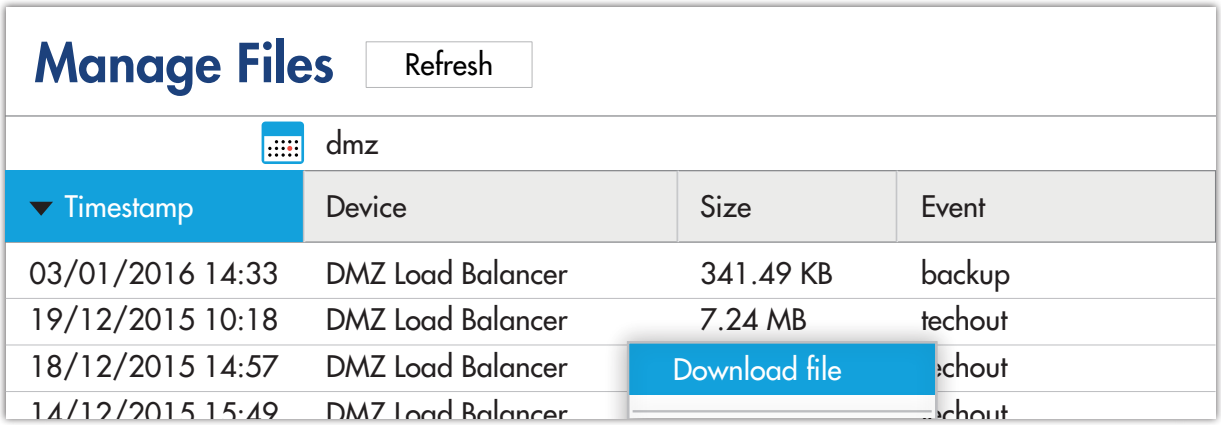
Device Techouts
Collecting diagnostic technical information can be a tedious and time consuming task.
A Tech-out task solves this by connecting to a device, running a recognized set of commands to collect diagnostic information and then copying it back to Osirium. Tech-outs can be stored for future examination and comparison with current issues.

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.



A.14 SYSTEM ACQUISITION DEVELOPMENT AND MAINTENANCE

14.1 Security requirements of information systems (A.14.1)

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 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 Security in development and support processes (A.14.2)

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	The organization should supervise and monitor the activity of outsourced system development.

Osirium 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 real-time information on who is accessing and working on critical problems while they happen.

A.15 SUPPLIER RELATIONSHIPS

15.1 Information Security in supplier relationships (A.15.1)

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 has the ability to 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.

Osirium applies a least-privilege security posture, ensuring that each privileged role, particularly those out-sourced to 3rd party service providers, are given no more than the level of privileged necessary for them to fulfil their jobs.

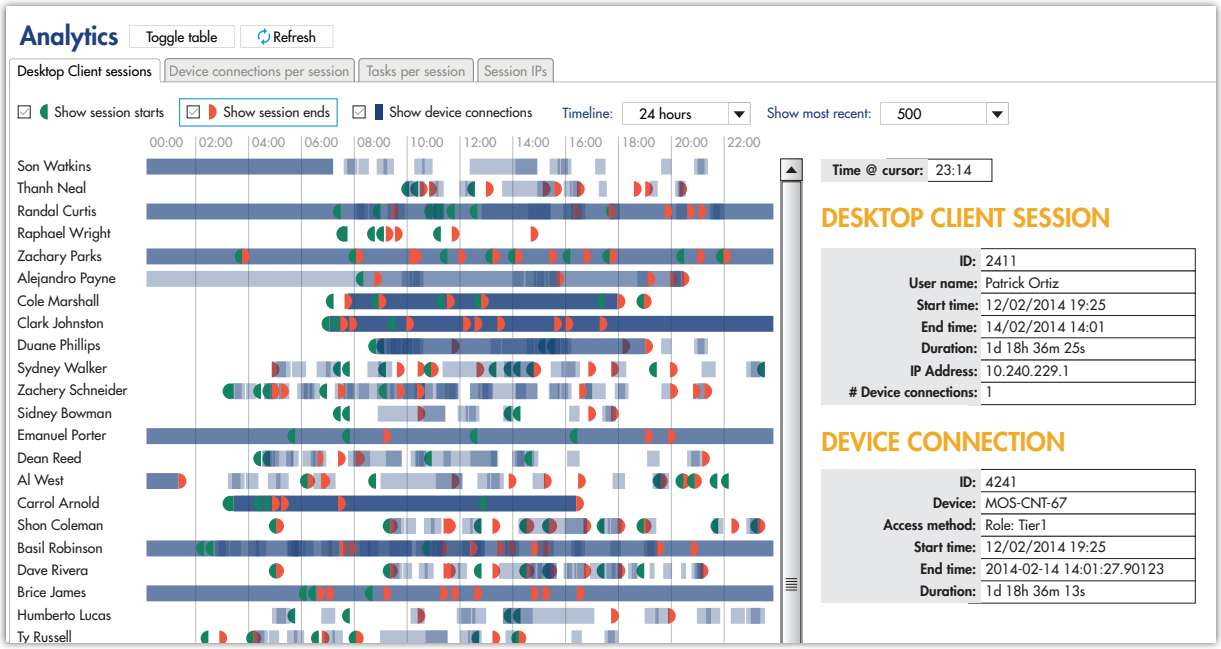
Time Windowed Access
3rd party access can be restricted to specific time windows, so whether overnight, at weekends or during routine daily maintenance, specific change windows can restrict write permissions to certain times.

Read-only access control can be also used to complement the restricted write access, allowing for in-house diagnostics and troubleshooting.

15.2 Supplier service delivery management (A.15.2)

15.2.1	Monitoring and review of supplier services	Organizations should regularly monitor, review and audit supplier service delivery.

Osirium allows monitoring and review of supplier services via Privileged Session Recording and privileged analytics.



A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 Management of information security incidents and improvements (A.16.1.)

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.

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.

ABOUT ACUITY GROUP

Established in 2006 and based in London, we are true specialists in the field, working with both national and international clients to deliver best practice integrated management systems. Our consultative approach ensures that the critical procedures we recommend - and put in place - exactly meet our clients' requirements. We are proud to be closely involved with British Standards as members of their ACP – Accredited Consultants Program.

Acuity Group exists to fulfil one objective, to make governance, risk management and compliance more accessible, more affordable and more profitable for all businesses.

Experienced in the delivery of ISMS and International Standards Compliance solutions on a global scale, Acuity Group is the ideal partner for any business looking to satisfy such objectives without unduly diverting its attention away from the strategic direction.

We differentiate ourselves by:

Fully integrated management systems.
International Standards (ISO) (Acuity Group Documented Methodology).

Web: acuitygroup.com Email: info.uk@acuitygroup.com Tel: +44 (0) 845 051 0361

ABOUT OSIRIUM TECHNOLOGIES PLC

In the current world of outsourcing it can be hard to see who has access to what on your systems. These days, the lowest paid people have the highest privileges - and they may not even work for your organisation. Osirium readdresses this balance for end-user organisations and uniquely allows MSSPs to manage tens of thousands of account credentials, outsource safely and keep their clients happy on the compliance front.

Our approach gives speed to value, enabling organisation see results as quickly as required.

Osirium prevents attacks on Privileged Accounts by separating people from passwords. Those privileged passwords never enter any workstation, they undergo Enterprise Class Password Life Cycle Management. We can build a least privileged model by removing the need for direct system access using Privileged Task Automation. Add Session Recording to allow you to see who did what, where and when.

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and password life cycle management, and then hand the pre-prepared session back to the incoming request ready for system management.

The session can be recorded, subject to time windows and device group separation. Osirium has delivered millions of privileged tasks and sessions for many of our blue chip clients.

Web: osirium.com Email: info@osirium.com Tel: +44 (0) 118 324 2444

OSIRIUM

11-13 High Street, Theale
Reading RG7 5AH

0118 324 2444
osirium.com