OSIRIUM WHITEPAPER

Achieving DSP Compliance with Osirium Privileged Access Security

Osirium PAS Shortens DSP Assessments

Accelerating DSP Assessments with Osirium

Introduction

The UK government made proposals in 2016 to improve cybersecurity within the NHS which led to the National Data Guardian introducing Digital Security and Protection (DSP) requirements in 2017. The DSP Toolkit has been created as an online tool for all affected organisations to show they are practicing good cyber and data security.

DSPT version 3 (the changes are listed here) is required for new assessments and makes Cyber Essentials a mandatory requirement for all relevant organisations. Osirium has a free whitepaper focused on achieving Cyber Essentials compliance, which is a good starting point for DSPT as many of the requirements of Cyber Essentials are foundations for DSP. In particular, the need for management of privileged accounts. That's not a surprise, after all, if you cannot control access to the security tools via administrator or other privileged accounts, then those tools are vulnerable.

Self-assessments must be completed annually and twice a year for those in category 1 and 2 – NHS Trusts and "Arm's length" bodies such clinical commissioning groups. Compliance is required of all service providers ranging from local authorities to GP practices and business partners. Every IT team is under pressure so can ill-afford time spent on collecting and submitting the required items of evidence, hence the urgent need for tools that can reduce or remove any manual effort.

That's where modern privileged access management (PAM) and automation is the solution. If the systems are in place to ensure policy compliance, they are being used and those tools can provide the necessary audit information, then DSPT submissions should be straightforward. This guide, based on the 2020 – 2021 standard, discusses the key elements of DSP that require PAM along with examples of how modern PAM and automation systems can be used to achieve compliance.

The DSP Compliance Challenge

Many of the requirements of DSP centre on human factors – training, awareness, etc. Clearly, they are important, but they depend on underlying technology to support those best behaviours. For example, it's one thing to train team members to use best practice for choosing passwords, but that should be supported by the systems being used to ensure compliance. Perhaps even more importantly, how are those policies implemented across hundreds or thousands of back-end and shared resources like databases, network devices or security tools?

Key Challenges for DSP Compliance

There are core capabilities required by many DSP requirements depend. The details are covered in a later section of this guide, but they can be summarised as:

COMMON CHALLENGE	PRIVILEGED ACCESS SECURITY SUPPORT
Governance of user credentials including adherence to password policies and removing access when no longer needed.	The heart of Privileged Access Security (PAS) is Privileged Access Management (PAM) which is the central visibility and control hub for all privileged access to shared devices, systems, and data. With this single point of control, policies can be implemented, enforced and audited.
Ensuring staff and partners can only access the systems they need and having control over what they do with that access.	As above, PAM provides that central control point to ensure users only have access to the systems they need. It also provides the option to watch, in real-time, what staff and partners are doing with the option to shutdown any inappropriate sessions. It also becomes the ultimate audit trail of who did what and when for auditing purposes or incident investigation.
Providing evidence for DSP compliance.	When the organisation spans many sites, there are hundreds of different servers, devices, applications and services to manage, collecting the required evidence to support a DSP audit is difficult and time-consuming. Using PAM as the gateway to all those systems and being confident it ensures policy compliance simplifies the process and reduces the load on the IT team for each assessment.

Compliance should only be the start

DSP compliance should not be just a box-ticking exercise. If done well, PAM and automation not only provides security for systems and data but can be a positive contribution to reducing manual effort, reducing cost, and improving service in everyday operations. For example:

Osirium PAM can allow partners or suppliers to safely access internal systems without needing complex remote access infrastructure while increasing visibility with real-time session monitoring.

Admins have faster access to the servers and systems they need through the Osirium PAM client – rather than having to find the right device in a list of hundreds or thousands, they only see the devices they are permitted to use. They can search for relevance devices (e.g. "Firewall in Manchester", and access credentials are injected by PAM so they're never exposed or shared. Risk is reduced, time is saved, and they can get on with their work.

The "MAP Server" in Osirium PAM, allows legacy applications to be accessed via a browser on any workstation or laptop, allowing the number of old, perhaps out of support systems, to be greatly reduced.

Osirium Privileged Process Automation (PPA), can be used to simplify management tasks so they can be safely delegated to IT help desk agents or end users (for example, regular tasks such as recertifying who has access to which systems).

About Osirium

Osirium is the leading UK-based vendor of **Privileged Access Security (PAS)** solutions. Osirium's cloud and on-premises 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 **Privileged Process Automation (PPA)** 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.

Using this guide

This guide takes the key elements of the DSP Toolkit requirements and shows how Privileged Access Security can be applied. There are other areas of the standard that can also benefit from PAM and automation but are out of scope for this guide. This guide refers to **"DSPT Requirements Specification for 2020 – 2021"** The standards are continually evolving, but these core principles should hold true for future releases of the standard.

DSPT Privileged Access Management Requirements

For the bulk of the assessment criteria, modern Privileged Access Management (PAM) and Privileged Process Automation (PPA) can make compliance easy and ensure on-going compliance. This guide will discuss how to use PAM and PPA to address the key requirements. There are some requirements outside the scope of PAS so, for simplicity, they've been omitted from the list.

If you'd like to know more about how to use PAM and PPA for a DSP assessment, please get in touch.

ASSERTION	EVIDENCE REF	EVIDENCE TEXT	HOW CAN OSIRIUM HELP?
Organisation assures good management and maintenance of identity and access control for it's networks and information systems.	4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	PAM provides a central audit point for all privileged access to shared systems, databases, and network devices.
	4.2.5	Are unnecessary user accounts removed or disabled?	Removing accounts can be an automated process in PPA as part of a standard "leaver's process." With access to privileged access managed by PAM, removing a user's access is a simple task in one system rather than the time-consuming and error-prone manual process of updating each system separately.
All staff understand that their activities on IT systems will be monitored and recorded for security purposes.	4.3.2	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Access to systems can only be made via the PAM system as the credentials are only held within PAM. Users must prove their identity before being able to use PAM. That proof may require Multi-Factor Authentication (MFA).
	4.3.5	Have all staff been notified that their system use could be monitored?	All or selected sessions can be recorded via the PAM system. When a recorded session starts, the user can be warned that the session is being recorded.
	4.4.1	Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged, and those logs are only accessible to appropriate personnel?	The PAM system maintains full audit trails of all sessions. Auditor can be granted limited access to review the logs as needed.

ASSERTION	EVIDENCE REF	EVIDENCE TEXT	HOW CAN OSIRIUM HELP?
You closely manage privileged user access to networks and information systems supporting the essential service.	4.4.3	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.	Protected servers should only have the applications needed to perform their work (i.e. no web browser or email client). PAM can further restrict access to specific applications via the "MAP Server". For maximum protection, automation can be used to ensure only specific functions are performed and the user cannot do anything they should not.
	4.4.4	The organisation only allows privileged access to be initiated from devices owned and managed by your organisation	Access to Osirium PAM can be managed rather than configuring access on every device, system or service.
	4.4.5	You record and store all privileged user sessions for offline analysis and investigation.	All privileged sessions are logged in the audit trail with additional recording of all screen and keyboard activity as required.
You ensure your passwords are suitable for the information you are protecting.	4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.	Privileged credentials managed by PAM can have policies and lifecycles enforced, for example, password complexity or rotation frequency. Because this is a machine-driven activity, it does not fall into the traps of poor password choice when humans must change passwords.
	4.5.3	Multifactor authentication is used [wherever technically feasible].	Multi-Factor Authentication via numerous methods can be requirement to prove the user's identity before gaining access to privileged systems.
	4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Privileged credential governance ensures passwords are changed when onboarding new systems and future updates follow prescribed policies.

ASSERTION	EVIDENCE REF	EVIDENCE TEXT	HOW CAN OSIRIUM HELP?
You ensure your passwords are suitable for the information you are protecting. (continued)	4.5.5	Does your organisation grant limited privileged access and third party access only for a limited time period, or is it planning to do so?	PAM allows access to external parties within selected time windows. Access is only granted to approved systems and all third-party access can be recorded.
	4.5.6	Do you have high-strength passwords defined in policy and enforced technically for all users of internet-facing authentication services?	PAM implements complex credential lifecycle policies for access to systems with privileged access.
All networking components have had their default passwords changed.	9.1.1	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password. planning to do so?	All new devices should have all their accounts managed by Osirium PAM so no default accounts will be left on the devices.
The organisation is protected by a well managed firewall.	9.7.1	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	Privileged Automation can be used to quickly and securely manage firewall rules and policies.
	9.7.2	Has the administrative interface used to manage the boundary firewall been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address?	All shared security systems, such as firewalls, should have all accounts managed by PAM to prevent unauthorised access.
	9.7.4	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Changes to firewalls can be automated by Osirium PPA to ensure policies are followed. They can include approval steps and full audit trails are maintained all approvals and changes.

Getting Started

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

To assess the effectiveness of PAM in addressing DSP requirements, a free version of Osirium PAM is available (via https://www.osirium.com/pam-express). Once you're 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.