OSIRIUM WHITEPAPER

Accelerating Cyber Essentials Compliance

Osirium Privileged Access Security Shortens Compliance Assessments

OSIRIUM

Accelerating Cyber Essentials Compliance

Introduction

The Cyber Essentials scheme has been developed by Government and industry to identify a set of standard requirements for mitigating the risk from the most common Internet-based threats. It's also the foundation for other regulatory standards such as the **Digital Security and Protection Toolkit (DSPT)**.

By implementing the required controls, and complying with the Cyber Essentials assurance framework, organisations should be able to mitigate against the majority of the most successful cyber-attacks targeting UK businesses. Besides being a set of best practice guidelines relevant to every organisation, it has also become a requirement for any business that wants to sell to the UK government.

Cyber Essentials concentrates on five key controls:

- Secure your internet connection
- Secure your devices and software
- Control access to your data and services
- Protect against viruses and other malware
- Keep your devices and software up-to-date

The basic level of Cyber Essentials is a self-certification that covers the basic requirements. Cyber Essentials Plus is recommended for most organisations as it requires a certified assessor to perform a technical audit of the five control areas. It also includes automatic cyber liability insurance for organisations with less than £20m annual turnover.

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 **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

Certification for Cyber Essentials Plus compliance is delivered by a network of experts (AKA “certification bodies”) across the country working with the IASME Consortium. Each certification body may have slightly different assessment questionnaires, but they all have very common requirements to assess capabilities in each of the five controls.

Many of the tests the assessors use cover general information about the business or other requirements which are out of scope for this document and have been omitted from the next section.

Cyber Essentials Assessment Criteria

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. Based on Osirium’s experience of being assessed for Cyber Essentials, this guide will discuss how to use PAM and PPA to address those common criteria. Question reference numbers and text may vary between assessors, but the descriptions should be sufficient to relate to your assessment document.

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

	QUESTION	HOW CAN OSIRIUM HELP?
A 2.9	Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers).	All network equipment should be provisioned in PAM and the built-in Inventory Report gives a detailed list of devices, including software versions.
A 4.2	When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices? How do you achieve this?	Provisioning the device in PAM and setting to the "Managed" state will automatically update the password from the default to a long complex random password compliant with your corporate policies.
A 4.3	Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess?	PAM enforces policies, including refresh cycles and password complexity. It can use long (anything up to 128 characters), random complex, 'unguessable' passwords.
A 4.4	Do you change the password when you believe it may have been compromised? How do you achieve this?	The Force Password Refresh option in PAM allows an immediate refresh of any chosen password.
A 4.5	Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case?	Often it is necessary to grant access to partners and suppliers. Provisioning a PAM system in a DMZ grants controlled access without allowing direct connection to the servers, devices or applications.
A 4.7	Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet?	A PPA or PAM task could be written to audit the firewall rule base and make sure their configuration matches this requirement. This task could be run on a schedule and automatic reports emailed out.
A 4.8	Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet?	A PPA or PAM task could be written to make sure the appropriate settings on each particular device block config access over the internet.
A 5.2	Have you ensured that all your laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of your business?	Osirium provide a free audit tool to uncover accounts on endpoints, especially those with administrator privileges.
A 5.3	Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?	A standard process for new devices is to add them to the PAM inventory and make them "fully managed" devices to ensure administrator accounts are controlled.
A 5.4	Do all your users and administrators use passwords of at least 8 characters?	A PPA task could report the password policy set in AD. PAM always uses longer than 8-character passwords.

	QUESTION	HOW CAN OSIRIUM HELP?
A 5.6	Do you ensure all users of these services use a password of at least 8 characters and that your systems do not restrict the length of the password?	A PPA task can report the password policy set in AD.
A 5.7	Do you ensure that you change passwords if you believe that they have been compromised?	PAM can refresh passwords on all devices when a breach is suspected.
A 5.8	Are your systems set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes?	PAM has this feature built-in for local user accounts.
A 5.9	Do you have a password policy that guides all your users?	PAM enforces password policies for shared devices. A PPA task could get and show the policy/policies to verify them.
A 6.1	Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?	A PPA task can check for outstanding updates on systems.
A 7.1	Are users only provided with user accounts after a process has been followed to approve their creation? Describe the process.	A PPA Task can be used to create accounts and also handle staff movements around the business. The task can require approval within PPA, without the need for an ITSM or PPA can be used to execute the changes once approved in the ITSM tool.
A 7.3	How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?	A PPA task can be used to process and action the deletion of leaver accounts with an audit trail to show the changes have been completed.
A 7.4	Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?	A PPA Task can be used to automate regular re-certification of user accounts and access.
A 7.5	Do you have a formal process for giving someone access to systems at an “administrator” level? Describe the process.	PPA can provide an automated workflow, including review/approval.
A 7.6	How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?	This is a classic PAM use case. As an example, we have a two-account model. Any staff that need admin access will use their second ‘username_admin’ account. They login to their workstation, email, browse the internet etc with their standard non-privileged user account

	QUESTION	HOW CAN OSIRIUM HELP?
A 7.7	How do you ensure that administrator accounts are not used for accessing email or web browsing?	This can be enforced with a PAM "two accounts" model. Only standard user accounts have email mailboxes and are permitted web browser access. Admin accounts don't have mailboxes, but there are times that admin accounts need internet access to download software package updates etc. All this access is logged.
A 7.8	Do you formally track which users have administrator accounts in your organisation?	PAM shows who has an admin account and what they can access. As well as historical data on their access.
A 7.9	Do you review who should have administrative access on a regular basis?	PAM gives a very clear view of who has access to administrator credentials, so it makes the review process simple. A PPA task automates the regular review and recertification process.
A 7.10	Have you enabled two-factor authentication for access to all administrative accounts?	Osirium PAM integrates with common MFA identity management systems to ensure the user requiring admin access is the right person before managing their access to the devices with admin credentials which are never exposed to the user.
A 7.11	Is this because two-factor authentication is not available for some or all of your devices or systems? List the devices or systems that do not allow two-factor authentication.	Implementing 2FA at the PAM means you only have to set it up once. And not have to setup on each and every device on the network. Doing this at the PAM massively simplifies achieving this point.

Getting Started

The first step to preparing for a Cyber Essentials 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 in addressing Cyber Essentials requirements, a free version of Osirium PAM is available (via https://www.osirium.com/pam-express). Once ready to consider a broader assessments, Osirium experts are available to discuss the options.

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