Security Standard – Patching & Exposure Management (SS-033)

Department for Work & Pensions

Chief Security Office

Date: 25/06/2026

This Patching & Exposure Management Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Authority are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

(Important note for screen reader users.) Paragraphs that contain a **'must'** statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains 'must' activities.

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

1. Table of Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	16/12/2019
1.1		Minor amendments in sections; 10.1.1 to cover automated patching 10.5.2 to cover both automated and manual patches 15. definition of endpoints.	26/08/2020
1.2		Added references to automated patching and immutable infrastructure in sections 8.3; 10.3.2; 10.3.3; 10.3.5; 10.4.1; 10.5.1; 10.5.2; Minor amendments in sections; 10.1.1 Greater emphasis on automated patching 10.1.3 Added applicability to manual patches 10.1.6 Added reference to evergreening modern infrastructure 10.2.3 Criticality/Timeframe amendments 10.2.4 Updated for zero day exploits 10.2.5 Further detail on dealing with emergency patches 10.3.2 Risk assessment, triage function and review requirements added 10.3.4 Specified that entitlement refers to manual patching 10.4.4 Added reference to Blue/Green deployment model.	15/01/2021

		10.5.4 Added reference to application updates 10.6.2 Added rationale for scanning Definition of terms updated Glossary updated	
2.0		Added NIST CSF references; Introduction – Added references to CIS v8 Controls Set; further information added regarding risk assessment and risk ownership. Scope – Clarification added to highlight that patching is only one component of vulnerability management. 11.1.4 Clarified application of security patches for new connections. 11.1.7 Differentiate between functional and security patches for delivery 11.2.2 Patch criticality changed to vulnerability; added a statement about assessing exploitability in addition to criticality. 11.2.3 Added statements about mitigating vulnerabilities to within risk appetite; added reference to medium vulnerabilities 11.6.4 Requirements added for coverage of reporting.	07/12/2022

2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years Compliance – Ref added to Security Assurance Strategy Scope: Applications, software, infrastructure, network & security appliances; environments 11.1.1 ‘should’ changed to ‘must’ 11.2.1 Threat intel from known, trusted third parties; trusted feeds; ‘should’ changed to ‘must’ 11.2.2 risk appetite, threat profile, exploitability; EPSS; prioritisation considering environmental factors; considered in triage 11.2.3 Critical vulnerability prioritisation criteria and timescales; independent monitoring function 11.2.4 High vulnerability timescales; independent monitoring function 11.2.5 Medium/Low vulnerability timescales; independent monitoring function 11.2.6 ‘should’ changed to ‘must’; supporting sources added 11.3.1 Systems to be assessed; relevant teams 11.3.2 ‘should’ changed to ‘must’; Incident/problem mgmt. processes and risk assessment	25/07/2024

		11.3.3 Risk register removed 11.3.4 Product 11.3.5 & 11.4.2 Types of repositories removed 11.4.3 Change mgmt. processes 11.4.4 Emergency patches 11.4.5 vulnerability triage process 11.4.6 Types of repositories removed 11.5.3 prioritisation that considers business criticality, exploitability, triage actions, risk analysis etc.	
3.0		Patching standard renamed to Patching & Exposure Mgmt standard Whole document and all security measures reviewed in line with updated Threat & Vulnerability Mgmt Policy Exceptions - updated Introduction - vulnerability & exposure mgmt; CTEM & AER; NCSC Scope – inclusion of vulnerability & exposure mgmt; exclusion of physical, personnel or process weaknesses; image management 11.1.1 And security updates 11.1.5 Full image rebuild 11.1.6 All systems connected to the network; immutable infrastructure requirements; software version levels 11.2.1 Exploits; continuous threat monitoring; automated tooling.	25/06/2026

		11.2.2 Vulnerability & exposure prioritisation methods; security testing outputs; EPSS must 11.2.3 Updated requirements with CTEM 11.2.4 Updated requirements without CTEM 11.2.5 Automated response actions 11.2.6 attacks against specific software versions 11.2.7 Contextual Risk validation 11.3 & security updates 11.3.1 Manual or automated assessment 11.3.2 Prioritisation; mitigation; Pre-Accepted Risk Decision 11.3.3 Automated tooling; reporting 11.3.4 Pre-defined decision making 11.3.5 Automated tooling 11.3.6 Exposure discovery 11.3.7 Mitigation pathways 11.3.8 Pre-accepted risk decisions 11.4.1 Manually applied patches 11.4.5 Refer to 11.2.3 & 11.2.4 11.4.7 Zero day mitigation 11.4.8 Image-based deployments and immutable infrastructure 11.5.2 Automated tooling 11.5.5 Prioritise infrastructure protection 11.5.6 Full image requirements 11.5.7 Image deployment	

		11.6 Update reporting requirements Internal refs - Unified Vulnerability Management (UVM) strategy; SS-003; SS-027 External refs - NCSC: Vulnerability management; Gartner Strategic Roadmap for Continuous Threat Exposure Management Abbreviations - additions Glossary - additions	

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	16/12/2019
1.1		Chief Security Officer	26/08/2020
1.2		Chief Security Officer	15/01/2021
2.0		Chief Security Officer	07/12/2022
2.1		Chief Security Officer	25/07/2024
3.0		Chief Security Officer	25/06/2026

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by 1st line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. D].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

(Important) this paragraph contains 'must' activities.

In this document the term **"must"** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Exceptions that permit the use of superseded images, unsupported software versions, or delayed upgrade cycles **must** be explicitly recorded as lifecycle risk exceptions, be time-bound, and be subject to enhanced monitoring and re-evaluation based on threat intelligence.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, technical engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications that manage security patching.

7. Accessibility statement

(Important) this paragraph contains ‘must’ activities.

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in **Error! Reference source not found.**F.

8. Introduction

(Important) this paragraph contains ‘must’ activities.

This standard has been updated and renamed to add requirements for managing vulnerabilities and the related exposure they present due to the increasing prevalence of AI-driven threats. This supports a move away from a purely patching-led approach towards Continuous Threat Exposure Management (CTEM).

In a mature CTEM environment, response timelines shift from periodic patching cycles to a continuous, risk-based approach often measured in days or hours for critical threats. To counter adversaries operating at machine speed, this standard formally enforces a ‘mitigate-first’ protocol, mandating that critical attack paths are rapidly neutralised via compensating controls.

Use of AI tools may be considered by organisations to discover previously undetected vulnerabilities for remediation, but this approach itself could create additional risks; NCSC have provided guidance on how to process and prioritise these, see ‘10 questions to ask when using AI models to find vulnerabilities’ [External References].

NCSC also advise that reducing the attack surface helps to respond to vulnerabilities and exploitation faster, by deploying additional controls on internet facing systems such as allow lists for VPN endpoints based on IP/geo-location, multi-factor authentication, privileged access management, identity governance etc.

As AI tools are being utilised to discover vulnerabilities at scale and at high speed, organisations with a high degree of ‘technical debt’ (a backlog of unresolved technical issues) may be particularly vulnerable to attack. Software vendors may thus roll out large numbers of patches and updates to counter this, known as a ‘patch wave’, NCSC have provided guidance on how to prioritise these most effectively, see ‘Preparing for a vulnerability patch wave’ [see External Refs].

To enable timely mitigation at machine speed, this standard supports the use of Automated Exposure Response (AER) capabilities. AER provides policy-constrained automation to contain, mitigate, or remediate exposures based on contextual risk, while maintaining clear accountability, auditability, and human-in-the-loop controls.

A mature CTEM program (often referred to in the context of CTEM v2 or advanced maturity) focuses on near real-time discovery and rapid mitigation.

In modern delivery models, exposure management increasingly centres on build artifacts, images, and deployment pipelines rather than individual hosts. As such, CTEM-driven remediation and Automated Exposure Response (AER) may act at the image or pipeline level to prevent vulnerable versions from entering or remaining in production.

Additional information can be found in NCSC guidance for Vulnerability Management and the Gartner Strategic Roadmap for Continuous Threat Exposure Management [see External References].

This standard thus defines the minimum technical security measures that **must** be implemented to secure Authority systems via vulnerability and exposure management, and security patching. It is also aligned to the overarching Technical Vulnerability Management Policy, [Ref. B] which details management of all technical vulnerabilities including patching.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NCSC, NIST, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third-party providers, such as the CIS Critical Security Controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.
The aim of this standard is to:

- ensure that patching requirements are clearly articulated and can be implemented consistently across the Authority and by third-party providers where applicable.
- mitigate risks and thus manage the exposure from common threats and vulnerabilities to an acceptable level for operation.
- Ensure that risk assessments include consideration of asset value and business criticality, with priority given to vulnerabilities that are exploitable both now, and in the future if threat intelligence indicates this.
- Ensure that identified risks are owned and managed by appropriate Risk Owners.
- support the implementation of security controls that enable the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and are enabled by the implementation of controls from the CIS Critical Security Controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure systems and services operated in the Authority or on behalf of the Authority are updated, maintained and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

This standard applies to all applications, software and infrastructure (including network and security appliances) in all environments (i.e. Production, Pre-Production, Test and Development etc.) within the Authority and supplier base (contracted third-party providers), for the purposes of delivering applications and services that handle Authority data.

It also supports the DWP Technical Vulnerability & Exposure Management Policy [Ref. B] which drives the requirements contained in this standard.

It should be noted that while physical, personnel, or process weaknesses fall outside this standard, system misconfigurations, compliance failures, and exposed architectural flaws are explicitly in scope. In alignment with the Authority's Unified Vulnerability Management (UVM) strategy [Ref. E], the remediation of insecure configurations is treated with the same urgency and governed by the same SLAs as traditional software patching.

This standard has been updated and renamed to include requirements for managing vulnerabilities and the related exposure they present, with the aim of reducing the overall risk to the Authority, which may be achieved through deployment of other controls, as part of effective risk management, which is highlighted in section 11.2.3.

This standard also applies to immutable infrastructure and image management, but via updates and upgrades rather than patching.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

(Important) this paragraph contains 'must' activities.

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

11.1 Security Patch Control Requirements

(Important) this paragraph contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Patching (including updates which fix security vulnerabilities) **must** be automated wherever possible and should utilise dedicated service accounts with elevated privileges where appropriate. Manual patching **must** only be conducted by users with enhanced access and/or privileged users in line with SS-001 – pt 2 Privileged User Access Security Standard [Ref. C].	PR.AA-05 PR.PS-02
11.1.2	Standard business users **must not** have the ability to install unauthorised patches on end points.	PR.AA-05 PR.PS-05
11.1.3	Any manually applied patches found to have bypassed control mechanisms for installation **must** be subject to a formal review and uninstallation if deemed necessary.	ID.RA-07 PR.PS-05
11.1.4	Upon connection to the production network, all systems **must** have up to date security patches applied to software or applications that are in vendor support.	PR.PS-01 PR.PS-02

11.1.5	For systems using immutable infrastructure, containers, or virtual machine images, remediation **must** be achieved through full image rebuild, validation, and redeployment rather than in-place modification. Accountable parties **must** implement image and artefact lifecycle controls, including: • Continuous scanning of build artefacts and images • Promotion gating based on exposure risk • Controlled promotion between environments • Automated retirement of superseded or vulnerable images. • Runtime systems **must** only execute approved images that meet the requirements of this standard. The patching and update process **must** ensure that both the offline (stored) and runtime virtual images are updated.	PR.PS-02
11.1.6	Patch levels **must** be maintained for the lifespan of all systems connected to the network. For modern infrastructure, this is achieved by 'evergreening' i.e. via continuous updates being applied. Systems, services, and deployment artefacts **must** be maintained on the latest vendor-supported versions. Operation at versions below the latest supported release (e.g. n-1 or older) **must not** be considered compliant by default. Where deviation is required, it **must** be risk-assessed, time-bound, subject to compensating controls, and immediately re-evaluated if threat intelligence indicates increased exploitability.	PR.PS-02 ID.AM-08

11.1.7	Patches that only deliver functional change and **do not** fix a vulnerability **must not** be delivered as security patches, although can be delivered via the same mechanisms at the same time.	ID.RA-07 PR.PS-02

11.2 Threat Intelligence and Response Timescales

(Important) this paragraph contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Threat intelligence from known, trusted third parties regarding system vulnerabilities and related exploits **must** be collected continuously. These **must** be analysed and processed promptly to determine risk and exposure to identify the appropriate mitigations. Automated tooling may be used to achieve this. During the assessment and monitoring phases of the incident workflow, Indicators of Compromise (IOCs) **must** be continuously captured, enriched, and recorded within Authority platforms. Assessments regarding threat network blocks and proactive containment directives **must** be rapidly disseminated via established IT service management workflows to ensure immediate execution by operational teams.	ID.RA-02 ID.RA-03 ID.RA-04 ID.RA-05

11.2.2	Vulnerabilities **must** be assigned a defined criticality, which may be determined using a variety of methods such as: • Validated security testing outputs, including ITHCs, penetration testing, red teaming, and continuous offensive security testing, **must** be treated as high-confidence exploitability indicators and **must** directly influence exposure prioritisation, SLA enforcement, escalation decisions, and automated containment actions. • Common Vulnerability Scoring System (CVSS) or where applicable, Common Weakness Enumeration (CWE) scoring calculations, where this is available (CVSS and CWE only provide a generic view on the criticality of discovered vulnerabilities, and do not take into account an individual organisation's security capability, risk appetite, threat profile, or the exploitability of a vulnerability in individual systems). • Exploit Prediction Scoring System (EPSS)) **must** also be used to augment this information, e.g. to assess exploitability to aid prioritisation, but this **must not** be used as the sole source of information in assessing risk. • The vulnerability is present in the 'CISA Known Exploited Vulnerabilities Catalog' [see External References]. The prioritisation of an exposure **must** be calculated using the Authority's Validation Formula (**Validation = Impact x Viability**) and	ID.RA-01 ID.RA-04 ID.RA-05 ID.RA-08

	contextualised against the **Operational Security Domains**: **Environment:** The demarcation of the asset (Development, Test, Stage, Production, Tooling). **Value:** The criticality of the asset to business operations (Levels 1 through 4). **Resilience:** The maturity of the deployed compensating controls surrounding the asset (Levels 1 through 6). **Exposure:** The immediate accessibility of the resource to threat actors (Low, Medium, High, Critical).	
11.2.3	For systems operating within an automated CTEM framework, remediation **must** adhere to timescales driven by Contextual Risk validation (see 11.2.7): • Critical: Immediate automated containment where feasible. The attack path **must** be mitigated (e.g., via WAF rules, port blocking, network isolation etc.) within 12 hours, and the vulnerability permanently eliminated (patched/upgraded) within 5 days of a patch being made available. To achieve the 12-hour mitigation SLA for Critical exposures in mature environments, vulnerability management teams **must** leverage the following automated response pathways upon successful Control Validation: Automated Self-Healing Infrastructure: Triggering dynamic reconfiguration of assets to a known-good state.	ID.RA-01 ID.RA-04 ID.RA-05 ID.RA-06

	CI/CD Pipeline Remediation: Pushing emergency mitigations directly through deployment pipelines. Automated Shutdown: Isolating or terminating the affected service/instance to kill the attack path • High**:** Remediated/mitigated within 7 days. • Medium/Low: Remediated/mitigated within 30 days. Where a permanent patch or upgrade is not immediately available, or deployment would introduce unacceptable operational risk, virtual patching controls may be deployed as an interim mitigation to neutralise the attack path. Virtual patching may include HIPS, WAF rules, IPS, or runtime exploit prevention controls and **must** be threat-driven, time-bound, continuously monitored, and not treated as a permanent substitute for remediation.	
11.2.4	For legacy environments and external suppliers unable to integrate with real-time CTEM telemetry, adherence to the following traditional patching SLAs serves as the mandatory minimum compliance level: • Critical: Patched within 7 days of an update being released. • High: Patched within 14 days of an update being released. • Medium/Low: Patched within 45 days of an update being released. In exceptional circumstances where these legacy timeframes cannot be met, the risk **must** be	ID.RA-04 ID.RA-05 ID.RA-06

	mitigated and formally accepted by an independent central monitoring function. To compensate for extended remediation timelines, legacy systems **must** be subjected to additional compensating controls. Systems communicating with legacy systems **must** implement strict, identity-based access controls to restrict the potential impact of unmitigated exposures.	
11.2.5	Automated response actions may be executed where pre-defined authority thresholds are met. Authority tiers **must** be defined and mapped to contextual risk, confidence, and potential impact: • Inform (notification only) • Remind (SLA prompting) • Warn (approval-gated mitigation) • Respond (pre-approved automated containment or remediation) Where risk exceeds delegated authority, or confidence is low, escalation to an accountable human decision-maker is mandatory.	ID.RA-06
11.2.6	Where threat intelligence indicates active exploitation against specific software versions, services running superseded or ‘n-1’ versions **must** be re-classified as higher-risk exposures, triggering accelerated mitigation or automated containment.	ID.RA-05

11.2.7	The following vulnerability characteristics **must** be considered as part of the Contextual Risk validation: • The vulnerability is exploitable via any attack vector (local, network, physical, adjacent) • The vulnerability is locally exploitable i.e. can be exploited with local access • The vulnerability does not require any authentication or bypasses normal user authentication (i.e. the user is not aware) • The vulnerability directly enables the execution of code on a vulnerable device • Exploit code is either publicly available or the existence of an exploit has been detected by other sources • The affected system(s) are in a sensitive area (i.e. Internet Facing, Network Security Zone with Critical Applications) • Any enterprise perimeter mitigations in place • Threat Intelligence indicating a heightened threat level.	ID.RA-05
11.2.8	Where applicable, the risk owner **must** consider advice on what mitigating actions can be taken to minimise the threat from zero-day exploits (which by definition do not have a patch available) from sources such as; • Threat Intelligence • Vulnerability Management • Security Architects • Engineering • Vendors/industry	ID.RA-05 ID.RA-06

11.3 Patch & Security Update Assessment

(Important) this paragraph contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	All patches and security updates **must** be assessed manually or via automated tooling.	ID.RA-04 ID.RA-06
11.3.2	Patching and the deployment of security updates **must** be conducted as standard but where patching is not feasible, the resulting exposure **must** be assessed within the service's overall security posture, considering; • service impact • compensating controls • threat context If the exposure is to be tolerated rather than remediated (aligning with the NCSC 'Acknowledge' status), it **must** be recorded in the Authority’s Risk Register. This record **must** detail a formally named Risk Owner who explicitly accepts the residual risk of exploitation. For image-based and immutable deployments, the assessment and resulting mitigation strategy **must** differentiate between lifecycle stages: • Build-Time: Where exposures are identified in build-time artefacts or images, mitigation **must** prioritise immediate rebuilds, promotion gating, or the blocking of the release. • Runtime: Where exposures are identified at runtime, mitigation **must** prioritise containment and isolation while image-level remediation is prepared.	ID.RA-04 ID.RA-05 ID.RA-06

11.3.3	A record of the decision to apply or reject manual patches, **must** be documented as part of the Risk Assessment process, and **must** be made available to the Office of the CSO. For automated patching (e.g. via updates), a record of the reason for rejecting a product update **must** be maintained and reviewed on a regular basis, along with a risk assessment. Automated tooling may be utilised to record this information.	ID.RA-07 PR.PS-02
11.3.4	The *entitlement* to patch a product manually **must** be confirmed before applying a patch e.g. open source products that do not have a support package or service wrapper. Automated tooling may utilise pre-defined decision making capabilities.	ID.AM-02 ID.RA-07
11.3.5	A record of all assets **must** be maintained along with their patch status, history, and next review date (which may be set as part of a regular, scheduled activity) where appropriate; automated tooling may be utilised for this purpose. For automated patching via upgrades, a record of the reason for rejecting a product update **must** be maintained and reviewed on a regular basis, along with a risk assessment.	ID.AM-02

11.3.6	Exposure discovery activities **must** include the continuous identification of assets and services within scope, including those that are internet-facing or externally reachable. To ensure comprehensive visibility, discovery activities **must** explicitly include the identification of systems, services, or deployment artefacts running superseded, deprecated, or unsupported versions, as well as retained or dormant images capable of re-deployment. To facilitate deep visibility into software supply chain exposures, accountable parties **must** generate, maintain, and continuously ingest Software Bill of Materials (SBOMs) for all internally developed and third-party applications and container images.	ID.AM-02 ID.AM-05 ID.AM-08
11.3.7	Following discovery and assessment, the mitigation pathway **must** be dictated by the lifecycle stage of the affected asset: • Build-Time: Where exposures are identified in build-time artefacts or images, mitigation **must** prioritise immediate rebuilds, promotion gating, or the active blocking of the release. • Runtime: Where exposures are identified in active runtime environments, mitigation **must** prioritise containment and isolation to neutralise the attack path while permanent image-level remediation is prepared and deployed.	ID.RA-05 PR.IR-01

11.3.8	A Pre-Accepted Risk Decision refers to the mandatory review of any historically approved risk acceptances during the 'Assess' phase of a current security event. This step ensures that prior business decisions to tolerate a specific vulnerability are actively re-evaluated against newly captured indicators of compromise (IOCs) or changes in the threat landscape, allowing the risk acceptance to be voided if the threat viability has increased. Furthermore, any Pre-Accepted Risk Decision is subject to immediate, event-driven re-evaluation. If continuous monitoring or threat intelligence identifies a significant shift in the exploitability of a previously accepted vulnerability (e.g., active exploitation in the wild), the standard 3-month review cycle is superseded. The risk acceptance decision is immediately voided, and the vulnerability **must** undergo an immediate security reassessment to agree on priority and define emergency mitigation actions, treating the issue with the strict urgency of a newly discovered critical exposure.	ID.RA-01 ID.RA-04 ID.RA-05

11.3.9	For systems operating within modern or cloud-native environments, authenticated web application scanning (DAST) **must** be integrated into the CI/CD delivery pipeline to gate production releases. For more information on CI/CD pipelines, please refer to SS-027 Security Testing standard [Ref. F] and SS-003 Secure Software Development Standard [Ref. G]. For legacy environments where pipeline integration is technically unfeasible, accountable parties **must** conduct authenticated web application scanning at least annually, and formally agreed by the Risk Owner. Authenticated web application scanning **must not** be performed on a live service to avoid any disruption.	PR.IR-01 DE.CM-09

11.4 Patch Testing

(Important) this paragraph contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	All manually applied patches **must** be tested in a suitable environment (meets live conditions) prior to being applied to the enterprise. This is also applicable to immutable infrastructure, which goes through a development environment and Continuous Integration pipelines. Where automated testing is employed, any remediation of vulnerabilities will follow the standard approach for software changes.	ID.RA-07 PR.PS-02
11.4.2	Accountable parties **must** test the patch to check for compatibility and integration, and create a back-up or restore point, which can be managed via version control or container repositories where appropriate. This detail must be documented.	PR.DS-11
11.4.3	The patch becomes approved once testing has been concluded satisfactorily.	ID.RA-07
11.4.4	Delivery of the approved patch across the estate **must** be in stages to reduce impact. The ‘Blue/Green’ deployment model can also be utilised to achieve this. This requirement may be waived in the case of emergency patches.	ID.RA-07 PR.PS-02
11.4.5	Approved patches **must** be applied across the enterprise in line with requirements described in sections 11.2.3 and 11.2.4.	ID.RA-05 ID.RA-06
11.4.6	Where testing is not feasible, this **must** be risk assessed.	ID.RA-06

11.4.7	For high-impact, zero-day vulnerabilities or those undergoing active exploitation, waiting for a tested vendor patch presents an unacceptable risk. Accountable parties **must** deploy immediate mitigating controls to neutralise the attack path before a permanent software patch is available. These mitigations may include virtual patching via approved host-based or application-level protection technologies where exploitation risk is high (e.g., WAF rules, HIPS), alongside network-level actions like port closure. Vulnerability Management Teams hold the authority to execute these defensive actions based on high-confidence threat intelligence alone.	ID.RA-02 ID.RA-04 ID.RA-05
11.4.8	For image-based deployments and immutable infrastructure, testing and approval **must** apply to the complete image or artefact, and not solely to the individual patches or packages contained within it. Accountable parties **must** validate the holistic stability and security of the rebuilt artefact prior to promotion.	PR.IR-01

11.5 Patch Delivery

(Important) this paragraph contains 'must' activities.

Reference	Minimum Technical Security Measures	
11.5.1	Where possible, accountable parties **must** automate patch deployment across end points. Immutable infrastructure is kept up to date continuously, via updates or upgrades, which achieve the same purpose as patching.	ID.RA-08 PR.PS-02

11.5.2	All patches, both manual and automated, **must** be recorded; automated tooling may be used to record this. For automated patching via upgrades, a record of the reason for rejecting a product update **must** be maintained and reviewed on a regular basis, along with a risk assessment.	ID.RA-01 ID.AM-02 ID.AM-08 ID.RA-07
11.5.3	Where appropriate, accountable parties **must** patch systems and end points based on their criticality and associated prioritisation that considers business criticality, exploitability, risk analysis etc.	ID.AM-05 ID.RA-05 ID.RA-06 GV.OC-05
11.5.4	Where appropriate, accountable parties **must** ensure all patching is applied across the enterprise where necessary. This includes applying application updates or upgrades that include security updates.	ID.AM-08 PR.PS-01 GV.OC-05
11.5.5	Delivery of mitigations and patches affecting enterprise edge infrastructure (e.g., VPN gateways or equivalents, firewalls) **must** be prioritised over internal assets. Technical controls **must** be implemented to ensure the strict logical and physical isolation of the device's management plane from the data routing plane, ensuring administrative interfaces are never exposed to untrusted external networks.	ID.RA-05

11.5.6	For systems deployed using immutable infrastructure, containers, or virtual machine images, the delivery of security mitigations and patches **must** be achieved through full image rebuild, validation, and redeployment rather than in-place modification. Accountable parties **must** ensure that only approved images meeting the requirements of this standard are promoted and deployed to runtime environments.	PR.PS-02 PR.IR-01
11.5.7	Delivery pipelines **must** enforce automated promotion gating to prevent the deployment of images or deployment artefacts that contain unmitigated critical or high-risk exposures. Plus, superseded, deprecated, or vulnerable images **must** be actively retired from repositories to prevent accidental re-deployment and the re-introduction of exposures.	PR.PS-02 PR.IR-01

11.6 Reporting

(Important) this paragraph contains 'must' activities.

Reference	Minimum Technical Security Measures	
11.6.1	When patches have been deployed on static infrastructure, reporting **must** be run to confirm their deployment. For immutable cloud infrastructure, reporting **must** confirm the successful deployment of the updated, secure image.	ID.RA-01 PR.PS-02

11.6.2	Automated scanning **must** be deployed to report on exposure status on a regular basis. In legacy environments, this will correlate patch status against vulnerabilities. In mature cloud environments, this **must** correlate current exposure posture and attack paths against active threats.	ID.RA-01 ID.RA-08
11.6.3	Patches that have not been implemented **must** be reported to the system and risk owner who remains responsible for the exposure caused by the inability to patch.	GV.RM-05 GV.RR-02 ID.RA-05
11.6.4	Vulnerability and exposure reporting **must** cover the entirety of the estate. However, metrics **must** be proportionate and tailored to the architectural environment. Static environments **must** report on absolute vulnerability counts and patch deployment SLAs. Highly elastic cloud environments **must** report on exposure posture, remediation velocity, and the mitigation of critical attack paths, acknowledging that raw vulnerability counts in ephemeral infrastructure fluctuate dynamically.	ID.RA-01

11.6.5	Where automated mitigation or remediation actions are executed, post-action verification **must** confirm exposure reduction, service health, and state synchronisation across security tooling, Configuration Management Databases (CMDB), and ITSM platforms. Automated rollback or fail-safe mechanisms **must** be configured to immediately revert changes if post-action verification detects severe service degradation. Evidence of this verification **must** be retained for assurance and audit purposes.	PR.PS-02 PR.IR-01
11.6.6	Reporting **must** include comprehensive visibility of version currency and image lifecycle state across the estate. This **must** explicitly include the number of systems, services, or artefacts operating below the latest vendor-supported version (e.g. n-1 or older) and track the age of retained images to identify dormancy risks.	PR.PS-02 PR.IR-01
11.6.7	All reporting **must** also be shared on request with the Office of the CSO.	GV.RR-02

12 Appendices

Appendix A. Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards which can also be cross referenced against the CIS Critical Security Controls set. [see External References]

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (Sub-category)	Related Security Measure
GV.OC-05	Outcomes, capabilities, and services that the organisation depends on are understood and communicated	11.5.3, 11.5.4
GV.RM-05	Lines of communication across the organisation are established for cybersecurity risks, including risks from suppliers and other third parties	11.6.3
GV.RM-06	A standardised method for calculating, documenting, categorising, and prioritising cybersecurity risks is established and communicated	11.2.2, 11.2.3, 11.2.4, 11.2.5
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	11.6.3, 11.6.7
ID.AM-02	Inventories of software, services, and systems managed by the organisation are maintained	11.3.4, 11.3.5, 11.3.6, 11.5.2
ID.AM-05	Assets are prioritised based on classification, criticality, resources, and impact on the mission	11.3.6, 11.5.3

ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.1.6, 11.3.6, 11.5.2, 11.5.4
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	11.1.6, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.3.8, 11.5.2, 11.6.1, 11.6.2, 11.6.4
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	11.2.1, 11.4.7
ID.RA-03	Internal and external threats to the organisation are identified and recorded	11.2.1
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.3.1, 11.3.2, 11.3.8, 11.4.7
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritisation	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.6, 11.2.7, 11.2.8, 11.3.2, 11.3.7, 11.3.8, 11.4.5, 11.4.7, 11.5.3, 11.5.5, 11.6.3
ID.RA-06	Risk responses are chosen, prioritised, planned, tracked, and communicated	11.2.3, 11.2.4, 11.2.5, 11.2.8, 11.3.1, 11.3.2, 11.4.5, 11.4.6, 11.5.3
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	11.1.3, 11.1.7, 11.3.3, 11.3.4, 11.4.1, 11.4.3, 11.4.4, 11.5.2
ID.RA-08	Processes for receiving, analysing, and responding to vulnerability disclosures are established	11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.5.1, 11.6.2
PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.1.1, 11.1.2
PR.DS-11	Backups of data are created, protected, maintained, and tested	11.4.2

PR.PS-01	Configuration management practices are established and applied	11.1.4, 11.5.4
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.2.3, 11.2.4, 11.2.5, 11.3.3, 11.4.1, 11.4.4, 11.5.1, 11.5.6, 11.5.7, 11.6.1, 11.6.5, 11.6.6
PR.PS-05	Installation and execution of unauthorised software are prevented	11.1.2, 11.1.3
PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.3.7, 11.3.9, 11.4.8, 11.5.6, 11.5.7, 11.6.5, 11.6.6
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.3.9

Appendix B. Internal references

Below, is a list of internal documents that **should** be read in conjunction with this standard.

Table 3 – Internal References

Ref	Document	Publicly Available*
A	DWP Architectural Blueprint	No
B	Technical Vulnerability Management Policy	Yes
C	SS-001 – pt 2 Privileged User Access Security Standard	Yes
D	DWP Security Assurance Strategy	No
E	Unified Vulnerability Management (UVM) strategy	No
F	SS-027 Security Testing standard	No
G	SS-003 Secure Software Development Standard	Yes

Requests to access non-publicly available documents **should be made to the Authority.*

Appendix C. External references

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

External Documents List
CIS Critical Security Controls set.
NIST – Cyber security Framework – 2018-04-16
NIST – 800-53 – Rev 5 – Security and Privacy Controls for Information
CISA Known Exploited Vulnerabilities Catalog
NCSC: Vulnerability management
Gartner Strategic Roadmap for Continuous Threat Exposure Management
NCSC: Preparing for a ‘vulnerability patch wave’
NCSC: 10 questions to ask when using AI models to find vulnerabilities

Appendix D. Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
AER	Automated Exposure Response	Industry term
CIS	Centre for Internet Security	Industry body
CMDB	Configuration Management Database	Industry term
CTEM	Continuous Threat Exposure Management	Industry term

CVSS	Common Vulnerability Scoring System - The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritise their vulnerability management processes.	Industry term
CWE	The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry.	Industry term
DDA	Digital Design Authority	Internal body
DWP	Department of Work and Pensions.	UK Government
GSCP	Government Security Classification Policy	UK Government
IOC	Indicator of Compromise	Industry term
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OS	Operating System	Industry term
OWASP	Open Web Application Security Project	Open source

Appendix E Glossary

Table 6 – Glossary

Term	Definition
Artefact	A build output produced by the software delivery pipeline, such as an image, binary, package, or archive, intended for deployment or execution.
Automated Exposure Response (AER)	The use of policy-constrained automation to contain, mitigate, or remediate security exposures based on contextual risk, while maintaining accountability, auditability, and human-in-the-loop controls.
Compensating Control	A control implemented to reduce risk when a primary control cannot be applied, typically used as a temporary mitigation pending permanent remediation.
Containment	Temporary, risk-reducing actions applied to neutralise an attack path or limit blast radius without permanently resolving the underlying vulnerability.
Contextual Risk	The level of risk a vulnerability poses considering factors specific to the environment, including the asset's business value, exposure, and existing resilience controls, rather than relying solely on generic severity scores.
Continuous Threat Exposure Management (CTEM)	A dynamic framework that expands beyond traditional software patching to continuously evaluate the visibility, accessibility, and vulnerability of digital assets to identify and mitigate genuine attack paths.
Dynamic Enforcement	The real-time adjustment of access, connectivity, or exposure controls based on current risk, threat intelligence, and system state.
Human-in-the-Loop (HITL)	A control mechanism requiring explicit human approval or intervention when risk, uncertainty, or impact exceeds delegated automation authority.
Image	A packaged, immutable artefact containing an operating system, runtime, application code, and configuration, deployed as a single unit (e.g., container image or VM image).

Image Lifecycle Management	The controlled process of building, scanning, validating, promoting, deploying, and retiring images or artefacts throughout their operational lifetime.
Image Retirement	The process of deprecating and preventing further deployment of superseded, vulnerable, or non-compliant images or artefacts.
Indicator of Compromise (IOC)	A forensic artefact or observable data point observed on a network or in an operating system that indicates a computer intrusion or malicious activity with high confidence.
Lifecycle Risk	Risk arising from the continued operation of systems, services, or artefacts that are deprecated, superseded, unsupported, or operating below the latest supported version.
'n-1' Version	A version one release behind the latest available supported version, which may increase exposure risk and requires explicit risk acceptance where used.
Offensive Security Testing	The use of adversary-led techniques, including penetration testing, red teaming, and continuous offensive security testing, to validate exploitability and exposure in real-world scenarios.
Patch	In the context of this document, a Security Patch or Patch is any fix that remediates a vulnerability within the system. Patches that only update or make functional changes are out of scope of patching. Patches that make both functional and security changes are in the scope of this document.
Emergency Patch	For the purposes of this document, these are typically out of cycle, irregular patches that have not yet been applied. They fix vulnerabilities that could have an enterprise-wide impact where there is clear evidence they are being actively exploited in other organisations, or, where the threat is deemed imminent, it is believed existing compensating controls will not provide mitigation.
Authorised patch	A patch authorised by a triage team which may or may not come from the vendor.

CVSS	Common Vulnerability Scoring System - The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organisations properly assess and prioritize their vulnerability management processes.
CWE	The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry.
End point	Servers, laptops, tablets, mobile phones, printers, multi-function devices, network device or other devices which connect to corporate networks.
IDS/ IPS	Intrusion Detection System/ Intrusion Prevention System.
ISM	Information Security Management.
Immutable Infrastructure	Immutable infrastructure is an approach to managing services and software deployments on IT resources wherein components are replaced rather than changed. An application or service is effectively rebuilt and redeployed each time any change occurs.
Blue/Green Deployment	Blue green deployment is an application release model that gradually transfers user traffic from a previous version of an app or microservice to a nearly identical new release. The old version can be called the blue environment while the new version can be known as the green environment. Once traffic is fully transferred from blue to green, blue can stand by in case of rollback or pulled from production and updated to become the template upon which the next update is made.
Evergreening	Evergreening refers to running services comprised of components that are always up to date. Evergreen IT encompasses not only the services at the user level, but all of the underlying infrastructures, whether on-site or outsourced.
Promotion Gating	The enforcement of automated controls that prevent the promotion or deployment of artefacts or images that do not meet defined security, exposure, or compliance criteria.

Risk Register	DWP ESRM Risk Register (GRC).
Vendor	A vendor patch is an update to a program provided by a software vendor to fix a problem with the software. A patch is typically a small update that does not significantly change the functionality. Typically, patches are deployed to fix bugs that have been discovered in a program, especially security vulnerabilities. The term distinguishes patches from the vendor from unofficial patches from users.
Version Currency	The state of a system, service, or artefact operating on the latest vendor-supported version available for its platform, runtime, or dependency.
Virtual Patching	The use of compensating technical controls, such as HIPS, WAF, IPS, or runtime protection, to block or mitigate exploitation of a vulnerability without applying a permanent software patch.
Zero Day Exploits	A zero-day exploit is a vulnerability (weakness) in software. It is called Zero-day because it is exploited before the vulnerability fix is made available by the vendor.

Appendix E. Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

DWP Accessibility Policy

DWP Accessibility Manual

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps