**University of the Sunshine Coast**

**Course Coordinator:** Shazi Saremi

Submission Due Date: 10/10/2025

SEC303 Device and Network Security

Assessment Task 2: Business Case for Implementing Essential 8 Level 2

## Table of Contents

**Author:**

Torin Flanagan (1169130)

Duc Nguyen (1158490)

Ainsley Baker (1163083)

Jett Schimming (1163748)

[Table of Contents 0](#_Toc210985427)

[Executive Summary 2](#_Toc210985428)

[Introduction & Context 3](#_Toc210985429)

[Understanding The Essential Eight 3](#_Toc210985430)

[Current Vulnerabilities 4](#_Toc210985431)

[Essential Eight Analysis 5](#_Toc210985432)

[Patch Applications 5](#_Toc210985433)

[Patch Operating Systems 6](#_Toc210985434)

[Multi-Factor Authentication (MFA) 6](#_Toc210985435)

[Restrict Admin Privileges 7](#_Toc210985436)

[Application Control 8](#_Toc210985437)

[Restrict Microsoft Office Macros 9](#_Toc210985438)

[User Application hardening 10](#_Toc210985439)

[Regular Backups 10](#_Toc210985440)

[Implementation Roadmap 11](#_Toc210985441)

[Conclusion 19](#_Toc210985442)

[Reference List 19](#_Toc210985443)

[Appendix List 21](#_Toc210985444)

# Executive Summary

EduNext must achieve NDES-2025 cybersecurity compliance within the next 12 months to maintain accreditation, protect government funding, and uphold stakeholder trust. With the organisation’s growing reliance on a cloud-based learning environment and AI-driven educational tools, EduNext’s cyber threat exposure has heightened, resulting with immediate and structured action deemed mandatory.

The ACSC Essential 8 framework provides a strategic and measurable approach towards accomplishing cybersecurity compliance. By integrating these eight mitigation strategies with Maturity Level 2 alignment, EduNext enhances resilience, strengthens system defences, and meets control requirements as outlined in the NDES-2025 standards.

Several critical vulnerabilities were identified by conducting cybersecurity assessments, each found requiring urgent attention. Student data remains at risk due to incomplete encryption standards and weak access controls across multiple systems, further creating potential avenues for unauthorised disclosure. Additionally, integrating AI technologies introduces new threats, with these including data misuse, and learning model manipulations, potentially compromising educational integrity. Insufficient MFA coverage across admin and cloud-based environments is another critical vulnerability, containing significant risks regarding account compromise. Furthermore, patch management delays extend essential system exposure to CVEs, heightening exploitation likelihoods and service disruptions.

To address such risks and accelerate compliance progress, several strategic top-level recommendations have been proposed to be implemented first as quick wins. It is required for EduNext to implement MFA across all user accounts, with prioritisation over privileged access, strengthening identity protection. Establishing automated patch management procedures is another top-level recommendation addressing all critical applications and OS, further ensuring timely vulnerability remediations and maintained system integrity. Deploying secured and routinely offline backups further guarantees data availability and recovery for if system compromise or data loss events ever occur. Finally, access control and privilege management is to be strengthened to minimise internal/external attack surfaces, resulting with users only granted permissions deemed necessary for the role.

By adopting the Essential 8 Level 2 compliance roadmap, EduNext will be positioned to meet NDES-2025 requirements efficiently and effectively. This initiative helps to safeguard student information confidentiality, mitigate AI and operational risks, and reinforce EduNext’s reputation of delivering secure and high-quality digital education. Ultimately, this compliance roadmap provides stakeholder assurance towards EduNext beng committed with maintaining high standards regarding cybersecurity governance and resilience.

# Introduction & Context

EduNext Learning is shaping the future of education by supporting over 15,000 students through personalised, hybrid, and online learning focused on digital equity and future-ready skills. In 2025, the Department of Education introduced NDES-2025, mandating all education providers to adopt secure, AI-assisted, and data-compliant learning platforms within the next 12 months. These standards prioritise data protection, responsible AI use, accessibility, and real-time analytics, with non-compliance resulting in loss of accreditation and government funding. To meet these requirements, EduNext is adopting the ACSC’s Essential 8 at Level 2 maturity to address LMS vulnerabilities, defend against moderate cyber threats, and ensure compliance with NDES-2025. By implementing the Essential 8 Level 2 framework, EduNext will adopt stronger cybersecurity, robust data protection, and NDES-2025 compliance (ACSC, 2017).

## Understanding The Essential Eight

By implementing Essential 8 Level 2, EduNext’s cybersecurity posture strengthens against threats targeting the LMS environment (Microsoft, 2024). This framework provides layered defences, through eight key controls:

* **Patch Applications:** Regularly conduct vulnerability scans, remediate vulnerabilities, and remove unsupported software.
* **Patch Operating Systems (OS):** Apply the same scanning and remediation at the OS level.
* **Multi-Factor Authentication (MFA):** Enforce phishing-resistant MFA measures for all EduNext users, with all authentication events logged.
* **Restrict Admin Privileges:** Strictly controlled, validated, and segregated admin access with full activity logging.
* **Application Control:** Allow only approved software, apply Microsoft’s blocklist, and log execution events.
* **Restrict Microsoft Office Macros:** Disable or restrict macros, block unsafe sources, and prevent user security changes.
* **User Application Hardening:** Remove/disable vulnerable software, harden browsers, Microsoft Office apps, and PDF software, lock security settings, and centrally log all events.
* **Regular Backups:** Secure, test, and restrict access for backups to prevent unauthorised modification or deletion.

By applying each control, EduNext strengthens data protection, mitigates vulnerabilities, and ensures full NDES-2025 compliance (ACSC, 2017).

# Current Vulnerabilities

|  |  |
| --- | --- |
| **Technical Risks** | **Human Factors** |
| Patch Applications:   * LMS lack patch management. * Third-party applications serve create points of entry. * Exposed to web application attacks (e.g. insecure APIs).   Patch OS:   * Vulnerable OS versions. * Insecure configurations. * Exposed to system vulnerabilities (e.g. unauthorised access).   MFA:   * Legacy authentication (e.g. SMTP, IMAP4, POP3). * Use weak methods. * Lack of enforcement.   Restrict Administrative Privileges:   * Over-privileged roles inside (IAM). * Inadequate S3 bucket (object container) security. * Lateral/vertical movement exposure.   Application Control:   * No application whitelisting. * BYOD without MDM policies. * Removable media executions.   Restrict Microsoft Office Macros:   * Macros remain active. * Embedded executable malware. * Lacking macro policy enforcements.   User Application Hardening:   * Legacy protocols used. * MFA bypass. * Insecure browser settings.   Regular Backups:   * Lack encryption, being vulnerable to corruption and ransomware. * Off-site redundancy and immutability. * Local file storage. | Patch Applications:   * Delay/ignore updates. * Unaware of application risks. * Left outdated/vulnerable.   Patch OS:   * Delay/ignore updates. * Unaware of OS risks. * Left outdated/vulnerable.   MFA:   * Resist installing apps (e.g. Authenticator). * Share credentials (e.g. phishing). * Rollout not accepted.   Restrict Administrative Privileges:   * Demand higher privileges. * Insider threats. * Data misuse or accidental change.   Application Control:   * Download unapproved applications. * Bypass whitelist restrictions. * Introduce malicious software.   Restrict Microsoft Office Macros:   * Install unauthorised browser resources. * Expose user credentials. * System corruption.   User Application Hardening:   * Install unauthorised browser resources. * Disable security settings. * Expose accounts.   Regular Backups:   * Work saved to unapproved locations. * Accidental deletion or mismanagement. * Lack backup policy understandings |

# Essential Eight Level 2 Analysis

## Patch Applications

Timely application patching, prompt vendor update installation, and regular vulnerability scanning will collectively strengthen EduNext system security, close potential security gaps, and significantly reduce exploitation risks, data breaches, or unauthorised access (Cyber Guys, 2013).

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Automated asset discovery. | Fortnightly. |
| Vulnerability scans. | Online services daily.  Productivity tools, browsers, PDF readers, and security products weekly.  All other applications fortnightly. |
| Vendor patches. | Critical within 48 hours.  Non-critical (online services/core apps) within 2 weeks.  All other updates within 1 month. |
| Unsupported applications. | Remove or replace immediately. |

(ACSC, 2017)

EduNext’s core vulnerabilities include the lack of a centralised patch management system, reliance on third-party tools like Zoom, Turnitin, and Azure AD, and limited vulnerability scanning, leaving key systems exposed to attacks such as SQL injection, XSS, and insecure APIs. Human factors, including users ignoring update prompts or delaying manual updates, further increase the risk of outdated and insecure applications.

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Rapid vulnerability detection protects student data and ensures NDES-2025 compliance. |
| Timely updates prevent core, third-party, and pilot services exploitation. |
| Regular patching improves accessibility, uptime, and system reliability. |
| Following Essential 8 Level 2 strengthens compliance, accreditation, and stakeholder trust. |
| Limitations | Patches will cause system downtime and unavailability. |
| Legacy software may require time-consuming and costly replacement. |
| Users may experience post-update issues, necessitating extra training. |

For NDES-2025 compliance, EduNext must implement a centralised patch management solution integrating Azure AD with AWS, including automated asset discovery, scheduled vulnerability scanning, and a patch-testing sandbox. Mandatory patching policies will enforce timely updates for all vulnerabilities, decommission unsupported software, and ensure staff and students are trained on compliance, privacy, security, AI fairness, etc.

## Patch Operating Systems

The purpose of patching OSs is to ensure vulnerabilities are identified and remediated to maintain system security. Regular device scanning, timely patches, and replacing unsupported OS versions is typically involved to minimise cyber threat exposures (e.g. viruses). In turn, OS patching will ensure EduNext’s LMS, staff endpoints, and BYOD devices will stand OS-level resilient, supporting operational continuity and strengthen data protection.

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Automated asset discovery. | Identify all environment devices, tracking patch status. |
| Vulnerability scans. | Internet-facing systems daily.  Internal devices fortnightly. |
| Critical patch application. | Apply critical OS patches within 48 hours. |
| Non-critical patch application. | Apply non-critical patches within 2-4 weeks. |
| Unsupported OS replacement | Replace any legacy/unsupported OS versions. |

EduNext currently contains unpatched/outdated OS versions across BYOD devices, staff endpoints, and AWS-hosted LMS servers. These unpatched configurations present significant vulnerabilities, increasing unauthorised access, malware infection, and privilege escalation risks, as outlined by MITRE ATT&CK. Such risks are exacerbated by user behaviours, with staff and students frequently delaying or ignoring updates, leaving systems more exposed. Additionally, vendor support for legacy devices in STEM hubs may no longer be available, further compounding security risks associated with outdates OSs.

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Reduce ransomware, breach, and exploitation risks. |
| Protects student data privacy and ensures LMS resilience. |
| Supports NDES-2025 compliance and cybersecurity frameworks. |
| Limitations | Patching may disrupt teaching and learning activities. |
| Enforcing updates on BYOD devices can be challenging. |
| Legacy systems may no longer support patches, requiring replacements. |

It is recommended that EduNext implement automated patching using AWS Inspector and Microsoft Endpoint Manager, scheduling updates outside of teaching hours to minimise disruptions. Any unsupported or legacy devices should be replaced, as they no longer recieve security updates, leaving systems vulnerable to exploitation and non-compliant with frameworks such as NIST SP 800-53 (NIST, 2020). Additionally, Azure AD conditional access should be enforced to block outdated or unpatched systems from accessing EduNext resources.

## Multi-Factor Authentication (MFA)

MFA provides a layered defence by requiring two or more types of verification, such as something you know (password), have (hardware token), is (biometrics), or does (behavioural patterns). Combining these factors diversify authentication and significantly reduces the risk of unauthorised access, even with compromised credentials (Kosinski, 2024).

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Full coverage. | MFA must be implemented for all accounts including staff, students, parents, and third parties. |
| Phishing-resistant methods. | Use FIDO2, passkeys, or hardware tokens to prevent credential theft. |
| Centralised logging. | All authentication events are centrally logged, maintained, and analysed. |
| Modernise legacy protocols. | Disable or update legacy protocols that can bypass MFA (IMAP, POP3, SMTP). |
| Accessibility. | Provide alternative MFA options for users with disabilities or device constraints. |

(ASD, 2017), (Lacey, 2024)

EduNext currently doesn’t mandate MFA across all accounts, leaving certain systems exposed to credential theft. Logging of sign-ins and MFA events is insufficient, reducing threat detection and response abilities. Legacy protocols remain active, allowing attackers to bypass MFA. Lastly, some users may resist adopting MFA or face compatibility issues with older devices.

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Strong protection against credential theft. |
| Phishing resistant authentication methods. |
| MFA enforced on all accounts, protecting company assets and data. |
| Diverse authentication methods cater for student needs. |
| Part of the Microsoft suite allowing for easy integration |
| Limitations | Legacy protocols must be blocked or modernised which could misconfigure systems reliant on it. |
| Hardware keys if used may add to costs. |
| Some BYOD devices if older can hinder MFA security against phishing. |
| Diverse range of users may find it difficult to adopt and be resistant to change. |
| Users with disabilities may not be able to use some methods requiring alternatives or fail-over. |

EduNext should enforce MFA organisation-wide using phishing-resistant methods such as FIDO2, passkeys, or hardware tokens, while also disabling or updating legacy protocols to prevent bypass. Centralised logging and monitoring are recommended, with accessibility measures and user training provided to ensure adoption and timely threat response.

## Restrict Admin Privileges

Admin privileges grant EduNext staff elevated rights for tasks like account management, file access, and system configuration, where securely restricting these rights is essential against adversary tactics (ACSC, 2017). By utilising the PoLP, access becomes limited to what is required for specific tasks (Billoir et al., 2024). In addition, RBAC policies further enforces restriction by assigning users roles aligned with operational needs, all remaining under admin oversight to reduce privilege escalation (Dekker et al., 2017).

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Approval and assignment. | Admin rights approved upon request and use dedicated accounts. |
| Monitoring and logging. | Centrally log activity for detection/response. |
| Revalidation and expiry. | 12-month account expiration or disabled after 45-day inactivity. |
| Environment isolation. | Admin accounts separated from unprivileged environments. |
| Access restrictions. | Unnecessary internet and email access restricted. |

(ACSC, 2017)

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Restricting admin rights reduces privilege escalation, lateral movement, and attack surface. |
| Limits sensitive data access, ensures accountability, and supports compliance. |
| Prevent unauthorised AI changes and preserves learning analytics accuracy. |
| Centralised logging and segregated environments improve incident response and reduce disruption. |
| Limitations | Requires investment in tools, monitoring, and administration. |
| Account switching may slow workflows and require staff training. |
| Misconfigurations or resistance may delay tasks and risk lockouts. |

Shared admin credentials, lack of revalidation, and no expiry controls leave accounts vulnerable and difficult to audit. Admins using same accounts for teaching and administrative tasks, along with unrestricted internet and email access, increase risk exposures. Weak credential management, unsegregated privileged environments, and absent centralised logging further expose systems to long-term compromise and delayed incident detection.

To meet NDES-2025 and Essential Eight Level 2 requirements, EduNext must implement dedicated admin accounts with PoLP via RBAC, restrict unnecessary access, segregate environments, enforce account revalidation and expiry, and use strong credential management with Azure AD PIM. Centralised logging, monitoring, and staff training will enable rapid incident detection, compliance, and minimise disruption to teaching and administrative operations.

## Application Control

Application control prevents unauthorised executables from running on systems by allowing only approved applications to run (ASD, 2011). Level 2 maturity requires enforcement across all workstations and internet-facing servers, user profiles, and system folders, by using Microsoft’s recommended blocklists, comprehensive logging, and annual rule validations (ASC, 2017).

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Application control enforcement. | Across all workstations, internet-facing servers, user profiles, and system folders. |
| Blocklist implementation. | Use Microsoft’s recommended blocklists for untrusted executables. |
| Logging | Comprehensive logging of allowed/blocked application events. |
| Policy validation. | Annual review and validation of application control rules. |
| BYOD management. | Enrol devices in MDM for enforcement. |

EduNext currently lacks application control, leaving its systems exposed to malware and unauthorised software execution. BYOD devices are unmanaged and not enrolled in a MDM solution, allowing users to freely download and run code from writable locations, including removable media (Microsoft, 2025).

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Aligns with NDES-2025 requirements of ensuring student data privacy by blocking unauthorised software and executables thereby reducing the threat of malware execution. |
| Comprehensive control of executable execution using policies. |
| In-depth logging of allow and deny events. |
| The risk of BYOD devices is reduced through MDM management. |
| Limitations | Deployment of WDAC/SELinux policies require comprehensive planning, labour and time to ensure all software utilised within EduNext’s enterprise is accounted for. |
| Users may be resistant to applications being locked down. |
| Ongoing maintenance of policies and rulesets to align with level 2 maturity. |
| Coverage gaps for certain BYOD devices such as macOS requiring more stringent controls. |

EduNext should implement Windows Defender Application Control on all windows endpoints and manage it centrally via Intune App Control for Business to allow only approved applications and enforce conditional access (Microsoft, 2025). SELinux should be deployed in enforcing mode on LMS and AI engines hosted on AWS to restrict process and user access to critical resources (Roy, 2024). Both solutions provide comprehensive logging of allowed/blocked execution events, ensuring executions are managed. Combining both ensures NDES-2025 and Essential 8 Level 2 compliance, ensuring only trusted applications are used across EduNext’s environment.

## Restrict Microsoft Office Macros

Microsoft Office macros are a common attack vector, allowing malicious payloads to execute within seemingly harmless documents (Australian Cyber Security Centre, 2024). Level 2 maturity requires macros to be disabled by default unless there is a documented business need, with permissions granted only to specific applications. All macro activity should be centrally tracked, revoked when unnecessary, and supplemented with AV scanning and user awareness to prevent exploitation.

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Macro default setting. | Macros must be disabled unless documented business need exists. |
| Permission control. | Grant access only to approved users/applications and centrally track. |
| Block internet macros. | Files from internet must have macros blocked. |
| AV scanning | Runtime AV scanning enforced for all macro-enabled documents. |
| Security settings. | Users cannot modify macro security settings without admin approval. |

(Microsoft, 2024)

EduNext is exposed to malware and ransomware through active or poorly managed macros, especially from internet or email sourced documents. In June 2024, Ukrainian attackers used an Excel VBA macro to deploy a multi-stage malware campaign with a Cobalt Strike payload (The Hacker News, 2024). Victims were tricked into enabling macros, allowing the malware to execute via regsvr32 and fetch DLLs to escalate the compromise. This highlights the need for EduNext to centrally manage macro controls to prevent breaches and lateral movement.

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Reduces phishing and malware risks. |
| Protects sensitive student and staff data. |
| Ensures Essential 8 Level 2 and NDES-2025 compliance. |
| Centralised tracking improves incident response. |
| Limitations | Requires carful policy management to avoid disrupting legitimate workflows. |
| Users may attempt to bypass restrictions. |
| Legacy documents may require macros. |
| Initial Intune/group policy setup and continue monitoring can be resource intensive. |

EduNext should enforce macro restrictions via Microsoft Intune and group policy, keeping macros disabled by default and granting access only to approved users under documented justifications (Australian Cyber Security Centre, 2024). Runtime AV scanning, continuous monitoring and user training should complement these controls to reduce phishing and ransomware risks and ensure compliance with Essential 8 Level 2 and NDES-2025.

## User Application hardening

User Application Hardening focuses on reducing the exploitation of commonly used applications such as browsers, Microsoft Office, and PDF software. This involves disabling insecure features, blocking risky behaviours, and enforcing strict security configurations across all user endpoints to protect against malware, phishing, and lateral movement attacks.

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Disable insecure features. | Unsafe functionalities must be turned off (e.g. legacy plugins). |
| Apply vendor security guidance. | Ensure applications follow strict vendor-recommended security settings. |
| Block suspicious behaviours. | Restrict unsafe and high-risk application behaviours. |
| Logging and monitoring. | Centralise logging of security events for rapid incident response and auditability. |

(ASD, 2017)

EduNext staff and students frequently install unauthorised browser extensions or disable security settings, exposing endpoints to account compromise and malicious executions. Legacy protocols and inconsistent logging further reduce visibility and hinder timely incident response, leaving LMS, AI grading tools, and student portals at risk of exploitation (Muncaster, 2025).

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Strengthens privacy and AI security. |
| Reduces phishing and malware risks. |
| Supports compliance with NDES-2025. |
| Improves incident detection and response. |
| Limitations | Restricting browser or Microsoft Office settings may frustrate staff. |
| Disabling legacy protocols could disrupt older integrations or systems. |
| Users may resist stricter application policies. |
| Enforcement requires ongoing monitoring and maintenance. |

Apply the ASD hardening baseline across all user applications and enforce Group Policy to block insecure browser settings. Disable legacy protocols and implement stricter rules around application installations. Ensure centralised logging is secure and efficient to enhance incident response, detection, and escalation processes.

## Regular Backups

Performing regular backups is a core cybersecurity measure to ensure EduNext can recover critical data and systems in the event of ransomware attacks, accidental deletion, or outages. Backups provide continuity and resilience, allowing restoration to a known point in time and safeguarding sensitive educational data.

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| Backup frequency. | Data, applications, and settings must be backed up according to business criticality and continuity requirements. |
| Synchronisation. | Backups must be synchronised to allow restoration to a common point in time. |
| Security and retention. | Must be secure, resilient, protected, from tampering or deletion, and retained for required periods. |
| Testing and recovery. | Backup restorations must be tested thoroughly before live incidents occur. |

(Australian Cyber Security Centre, 2024)

EduNext’s LMS hosted on AWS currently lacks regularly tested backups, placing grades, student records, and course materials at risk during outages or ransomware attacks. New systems such as AI-assisted essay grading and VR-based learning introduce additional data sources that may not be included in existing backups. Limited disaster recover testing creates gaps that could lead to permanent data loss and jeopardise NDES-2025 compliance.

|  |  |
| --- | --- |
| **Category** | **Description** |
| Benefits | Ensures recovery from ransomware, deletion, or outages. |
| Protects sensitive student and staff data. |
| Supports NDES-2025 compliance. |
| Enhances disaster recovery and business continuity. |
| Limitations | Implementing and managing comprehensive backups requires resources and planning. |
| Backup testing may temporarily impact system performance. |
| BYOD or third-party data sources may complicate complete coverage. |
| Requires ongoing monitoring and maintenance to ensure reliability. |

EduNext is to adopt the 3-2-1 backup model, this incorporating three copies on two media types, with one offline or offsite, while also using encrypted and immutable backups with strict access controls. Annual recovery exercises should include full system restoration and post-test reviews to strengthen processes. Critical asset, including LMS data, AI datasets, Zoom recordings, and parent portal information, must all be included in the backup plan to ensure comprehensive coverage.

# Implementation Roadmap

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase and Timeline** | **Essential 8 Component** | **Key Actions** | **NDES-2025 Alignment** |
| Phase 1  Quick Wins  0–3 months | Patch Applications | Centralise patch management with Microsoft Endpoint Manager and run baseline vulnerability scans. | Quickly reduces attack surface, enables secure access via authentication and supports student data privacy.  Ensures uninterrupted access and strengthens accountability and compliance.  Directly supports student data privacy and continuity of teaching  Builds foundations for responsible technology use through policy enforcement and awareness.  Supports data reliability by ensuring critical systems are recoverable and enhances transparency through documentation of backup procedures.  Minimise threat surfaces by ensuring only approved software is executed ensuring privacy and security. |
| Patch OS | Deploy AWS Inspector and Endpoint Manage for LMS servers and staff devices. Establish patching timeline and schedule windows outside class hours. |
| MFA | Deploy MFA by turning on MFA across EduNext Tenancy enforcing it across all relevant stakeholders. Switch on logging across organisation with security alerts for abnormalities. |
| Restrict Administrative Privileges | Use Azure AD PIM for dedicated admin accounts and enforce PoLP with RBAC. |
| Application Control | Start Pilot group for Managed Installer with individuals from all roles to start testing application control via WDAC. Enforce MDM join across the organisation. AWS LMS/AI servers will enable and configure SELinux on test machine. |
| Restrict Microsoft Office Macros | Disable macros by default via Group Policy and Intune. Confirm that macros are blocked in files originating from the internet. Enable Microsoft Defender macro runtime scanning across all endpoints. Communicate initial policy changes to staff through awareness emails Enforce policy that users cannot modify macro security settings. |
| User Application Hardening | Use Group Policy to build baseline browser and Office security settings  Disable Internet Explorer on all EduNext devices. |
| Regular Backups | Review existing AWS and Microsoft 365 backup configurations. Implement basic encryptions for all current backups. Establish temporary off-site or cloud redundancy for priority data. |
| Phase 2  Mid-Term  3–6 months | Patch Applications | Enforce patch timelines and use an Azure DevTest Labs sandbox to reduce update disruptions. | Ensures timely updates, strengthens system resilience, minimises disruption, reduces privilege misuse, and supports compliance.  Strengthens communication channels and limits and prevents misuse.  Builds resilience in hybrid learning platforms.  Phishing resistant MFA options provide strengthened security ensuring data privacy.    WDAC testing and scaling ensures proper integration of a security component ensuring proper controls are in place for security. |
| Patch OS | Start replacing unsupported STEM hub devices. Block outdated OS logins using Azure AD conditional access. |
| MFA | Extend MFA across EduNext organisation ensuring phishing resistant methods and utilising SMS only as a fallback. |
| Restrict Administrative Privileges | Limit unnecessary internet/email access for admin accounts and monitor activity via Azure Sentinel. |
| Application Control | Expand WDAC to organisation. Extend pilot further with 30% of users adopting. Utilise Microsoft recommended blocklist  SELinux enforced on all LMS/AI nodes. |
| Restrict Microsoft Office Macros | Create an Active Directory security group for approved macro users. |
| User Application Hardening | Strengthen rules for browser extension installations and approved apps. Ensure the removal legacy email protocols. |
| Regular Backups | Formalise and automate secure critical system backups using AWS Backup with S3 Object Lock. Synchronise backup copies, introduce initial restoration testing, and implement access controls with immutability measures. |
| Phase 3 Expansion  6–9 months | Patch Applications | Automate patch deployment and monitoring in Microsoft Endpoint Manager, validating success and resolving failures. | Ensures consistent patching, addresses vulnerabilities, limits privilege escalation, and strengthens proactive security monitoring.  Supports real-time analytics for educators and proactive incident detection for cyber security  Allow list allows only approved tools to be run on AI nodes ensuring responsible and AI security. |
| Patch OS | Fortnightly patch compliance reporting for BYOD and internal servers. |
| MFA | Improve MFA with conditional access policies. Extend MFA to all applications. Centralise allow/deny logs for comprehensive logging and alerts. |
| Restrict Administrative Privileges | Automate admin account validation/expiry via Azure AD and segregate privileged from standard environments. |
| Application Control | WDAC to be expanded to 90% of users and strays are manually configured.  Configure SELinux with centralised and comprehensive logging and alerts. |
| Restrict Microsoft Office Macros | Test macro policy enforcement using simulated phishing attachments. |
| User Application Hardening | Increase logging and monitoring of PowerShell and command line activity. Centralise event analysis for AI-assisted alerting and end point detection. |
| Regular Backups | Implement the 3-2-1 backup model (three copies, two media types, one off-site). Expand backup coverage to include other assets such as AI datasets, zoom recordings and LMS analytics. Test partial system restoration. Encrypt all backups and enforce access restrictions for unprivileged accounts. |
| Phase 4 Audit & Certification 9–12 months | Patch Applications | Audit patch compliance, remediate vulnerabilities, and decommission unsupported or legacy applications. | Confirms patch compliance, mitigates risks, ensures accountability, and finalises Essential Eight Level 2 compliance.  Endpoint security is enforced approving only authenticated and approved applications ensuring accessibility as well as student data privacy and security.  Authentication across all platforms are logged and monitored for any abnormalities ensuring security, accessibility so that EduNext can continue operations as normal. |
| Patch OS | Penetration testing of EduNext servers  Audit and penetration test OS patching procedures.  Review of last 9 months of patches and adjust as needed. |
| MFA | Audit MFA, remove SMS fallback where possible and ensure only secure authentication is used. Ensure comprehensive logging and alerts are set up. |
| Restrict Administrative Privileges | Audit privileged accounts, remove inactive accounts, and review logs/incident response via Azure Sentinel |
| Application Control | Audit Application controls on WDAC and SELinux, ensure only approved applications are running. Re-correct any unapproved applications. |
| Restrict Microsoft Office Macros | Audit privileged accounts, remove inactive ones, and review logs/incident response via Azure Sentinel. |
| User Application Hardening | Audit Microsoft 365, browsers, and PDF tools security settings.  Review and validate centralised logging effectiveness. |
| Regular Backups | Audit and validate backup strategy through reviewing 9-month backup logs. |

# Conclusion

EduNext has clear gaps within their security, systems and infrastructure including, inconsistent or delayed patching, unsupported application versions, legacy or no authentication, over-privileged access, unsegregated admin access, no tenancy application control, permissible office macro settings, weak application hardening, and poor backups without regular tested recovery or immutability. These identified gaps leads EduNext’s systems and sensitive data vulnerable with the potential for disrupting teaching and resulting in reputational risks or compliance fines. Adopting the Essential Eight Maturity Level 2 will remediate the gaps through, timely vulnerability scanning then patching, MFA adopted across all users, least-privilege with segmented admin accounts alongside PIM, enforced application control through WDAC and SELinux, macro blocking controls, 3-2-1 immutable and encrypted backups that have been validated. Following the 12-month phased roadmap will ensure NDES-2025 compliance, significantly reducing malware, risk of data loss, and ensuring operational continuity safeguarding EduNext from reputational risks or financial loss, as well as maintaining stakeholder trust in a reliable learning environment.

# Reference List

Australian Cyber Security Centre. (2024, August). PROTECT – Essential Eight assessment process guide. Australian Government.

<https://www.cyber.gov.au/sites/default/files/2024-08/PROTECT%20-%20Essential%20Eight%20Assessment%20Process%20Guide%20%28August%202024%29.pdf>

Australian Cyber Security Centre. (2017). Essential Eight Maturity Model. Cyber.gov.au. <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model>

ASD. (2011). Implementing application control. https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Implementing%20Application%20Control%20%28October%202021%29.pdf

Billoir, E., Laborde, R., Wazan, A., Rütschlé, Y., & Benzekri, A. (2024). Implementing the Principle of Least Administrative Privilege on Operating Systems: Challenges and Perspectives.

Cyber Guys. (2013). The Essential 8 In Plain English.

CSF. (2021, March 5). Unsupported System Components - CSF Tools. CSF Tools - the Cybersecurity Framework for Humans. <https://csf.tools/reference/nist-sp-800-53/r5/sa/sa-22/>

Dekker, M. A. C., Cederquist, J., Crampton, J., & Etalle, S. (2017). Administrative Privileges in RBAC.

Kosinski, M. (2024, January 4). Multi-factor authentication. Ibm.com. https://www.ibm.com/think/topics/multi-factor-authentication

Lacey, K. (2024, November 21). Securing Microsoft 365: Avoiding Multi-factor Authentication Bypass Vulnerabilities. Kroll. https://www.kroll.com/en/publications/cyber/securing-microsoft-365-avoiding-multi-factor-authentication-bypass-vulnerabilities

Microsoft. (2024, August 2). ACSC Essential Eight. Microsoft Compliance. <https://learn.microsoft.com/en-us/compliance/anz/e8-overview>

Microsoft. (2025). Application control for windows. Microsoft.com. https://learn.microsoft.com/en-au/windows/security/application-security/application-control/app-control-for-business/

MITRE. (2024). MITRE ATT&CK®. Attack.mitre.org. <https://attack.mitre.org>

Muncaster, P. (2025). The hidden risks of browser extensions – and how to avoid them. Welivesecurity.com. <https://www.welivesecurity.com/en/cybersecurity/hidden-risks-browser-extensions/>

Roy, S. (2024, March 19). Baeldung. Baeldung on Linux. https://www.baeldung.com/linux/selinux-vs-apparmor

The Hacker News. (2024, June 4). Hackers Use MS Excel Macro to Launch Multi-Stage Malware Attack in Ukraine. The Hacker News. <https://thehackernews.com/2024/06/hackers-use-ms-excel-macro-to-launch.html>

# Appendix List

Appendix 1: Maturity Level 2 (ACSC, 2017)

|  |  |
| --- | --- |
| **Mitigation Strategy** | **Description** |
| **Patch applications** | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. |
| A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. |
| A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. |
| A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. |
| A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. |
| Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. |
| Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. |
| Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. |
| Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. |
| Online services that are no longer supported by vendors are removed. |
| Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed. |
| **Patch operating systems** | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. |
| A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. |
| A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. |
| A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. |
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. |
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. |
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release. |
| Operating systems that are no longer supported by vendors are replaced. |
| **Multi-factor authentication** | Multi-factor authentication is used to authenticate users to their organisation’s online services that process, store or communicate their organisation’s sensitive data. |
| Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation’s sensitive data. |
| Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation’s non-sensitive data. |
| Multi-factor authentication is used to authenticate users to their organisation’s online customer services that process, store or communicate their organisation’s sensitive customer data. |
| Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation’s sensitive customer data. |
| Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. |
| Multi-factor authentication is used to authenticate privileged users of systems. |
| Multi-factor authentication is used to authenticate unprivileged users of systems. |
| Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are. |
| Multi-factor authentication used for authenticating users of online services is phishing-resistant. |
| Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option. |
| Multi-factor authentication used for authenticating users of systems is phishing-resistant. |
| Successful and unsuccessful multi-factor authentication events are centrally logged. |
| Event logs are protected from unauthorised modification and deletion. |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. |
| Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. |
| Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. |
| **Restrict administrative privileges** | Requests for privileged access to systems, applications and data repositories are validated when first requested. |
| Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. |
| Privileged access to systems and applications is disabled after 45 days of inactivity. |
| Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. |
| Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. |
| Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. |
| Privileged users use separate privileged and unprivileged operating environments. |
| Privileged operating environments are not virtualised within unprivileged operating environments. |
| Unprivileged user accounts cannot logon to privileged operating environments. |
| Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. |
| Administrative activities are conducted through jump servers. |
| Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. |
| Privileged access events are centrally logged. |
| Privileged user account and security group management events are centrally logged. |
| Event logs are protected from unauthorised modification and deletion. |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. |
| Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. |
| Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. |
| **Application control** | Application control is implemented on workstations. |
| Application control is implemented on internet-facing servers. |
| Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. |
| Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. |
| Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. |
| Microsoft’s recommended application blocklist is implemented. |
| Application control rulesets are validated on an annual or more frequent basis. |
| Allowed and blocked application control events are centrally logged. |
| Event logs are protected from unauthorised modification and deletion. |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. |
| Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. |
| Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. |
| **Restrict Microsoft Office macros** | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. |
| Microsoft Office macros in files originating from the internet are blocked. |
| Microsoft Office macro antivirus scanning is enabled. |
| Microsoft Office macros are blocked from making Win32 API calls. |
| Microsoft Office macro security settings cannot be changed by users. |
| **Regular backups** | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. |
| Backups of data, applications and settings are synchronised to enable restoration to a common point in time. |
| Backups of data, applications and settings are retained in a secure and resilient manner. |
| Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. |
| Unprivileged user accounts cannot access backups belonging to other user accounts. |
| Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts. |
| Unprivileged user accounts are prevented from modifying and deleting backups. |
| Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. |