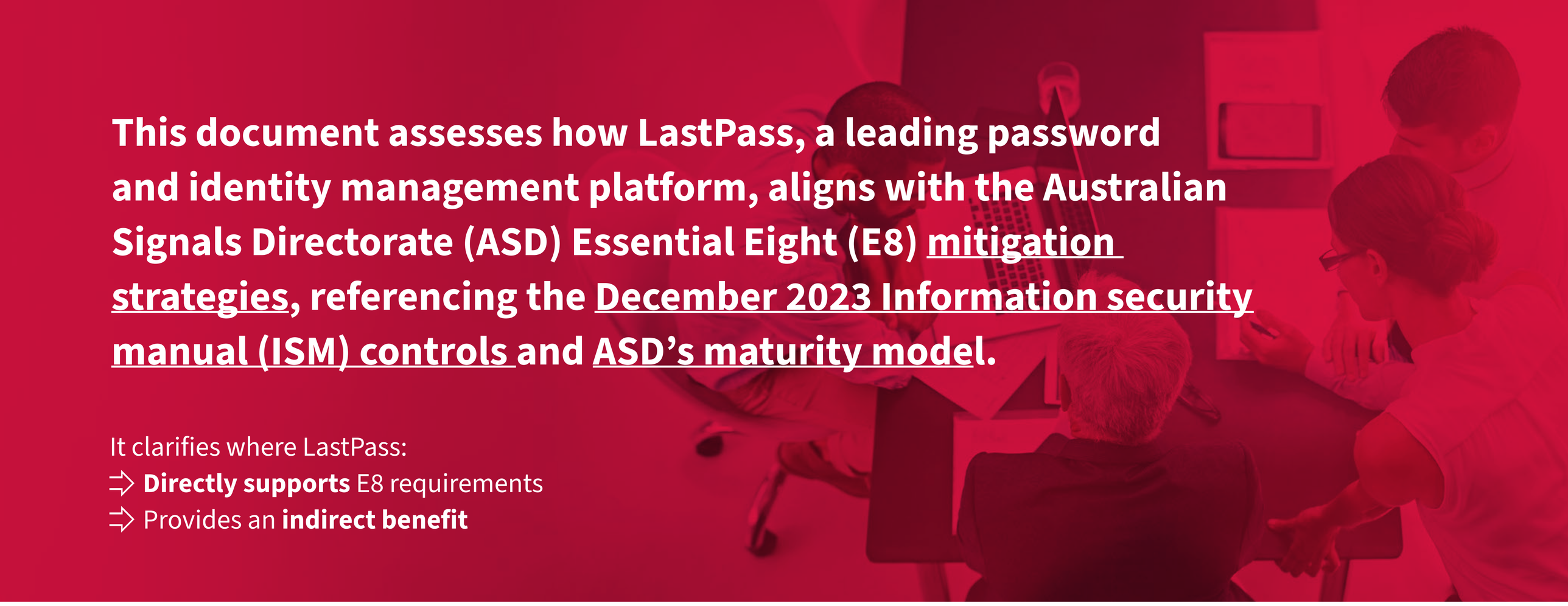
LastPass

LastPass and the Essential Eight:

Supporting Compliance with ASD's Maturity Model



This document assesses how LastPass, a leading password and identity management platform, aligns with the Australian Signals Directorate (ASD) Essential Eight (E8) mitigation strategies, referencing the December 2023 Information security manual (ISM) controls and ASD's maturity model.

It clarifies where LastPass:

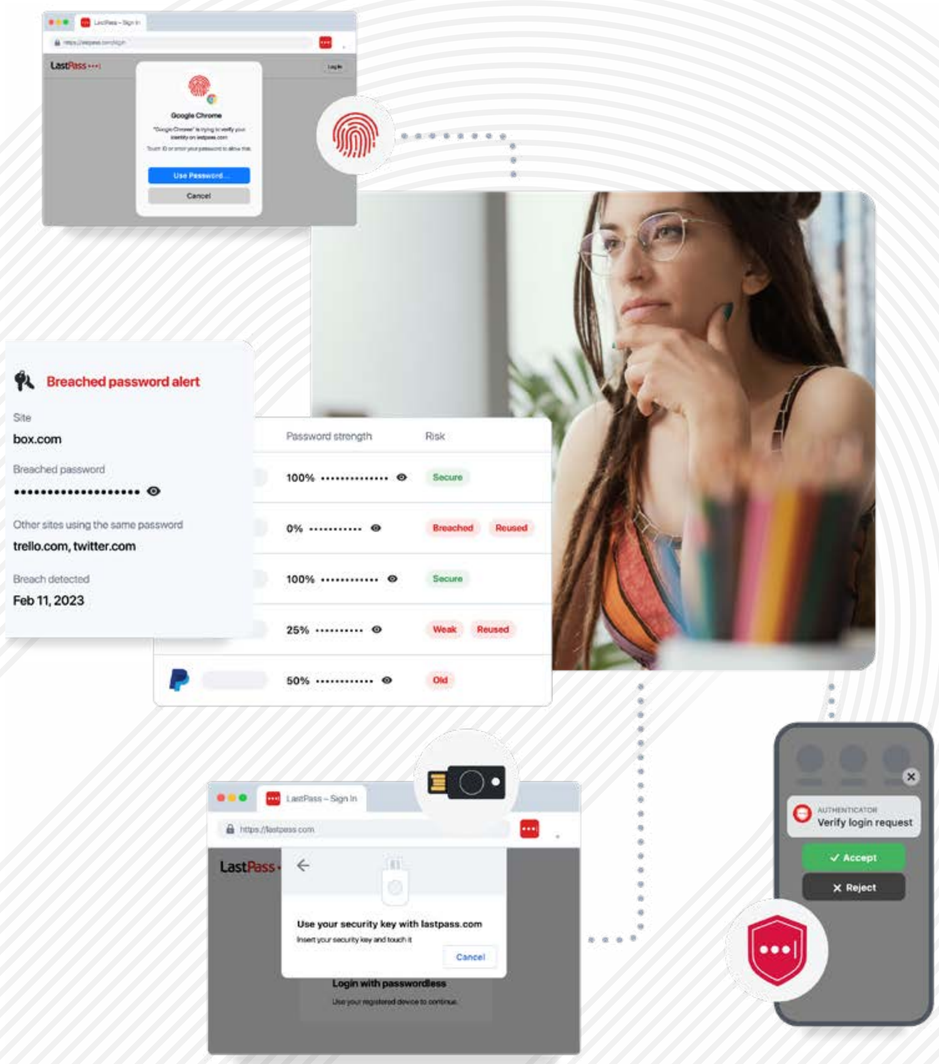
- **Directly supports** E8 requirements
- Provides an **indirect benefit**

This mapping also informs government and enterprise security architects of the strengths and boundaries of LastPass in uplifting cyber maturity of the ASD's maturity model (Levels Zero (minimum) through Three (maximum)).

Overview of LastPass Capabilities

LastPass is a cloud-based service offering:

- Encrypted credential vaults for individuals and teams
- Role-based access control (RBAC)
- Secure password sharing and policy enforcement
- Federated identity support and SSO integration
- Multi-factor authentication (MFA) with time-based one-time password (TOTP), push, and FIDO2/WebAuthn
- Software-as-a-Service (SaaS) application monitoring
- Admin policy enforcement and audit logging
- Secure recovery options for credential continuity



These features provide a strong foundation for identity and access controls across the Essential Eight.

It is important to note, however, that while this document outlines how LastPass supports elements of the Essential Eight maturity model, it does not imply that LastPass alone can achieve compliance. Broader system controls and enterprise integrations are required.

Control-by-Control Mapping

1. Patch Applications

Objective: Patch apps to address vulnerabilities

Relevant ISM Controls: ISM-0283, ISM-1712

Assessment:

Direct Support	Not provided. LastPass does not patch or manage applications.
Indirect Benefit	Vault-stored credentials streamline secure reauthentication and app access after patch cycles, reducing manual resets.
Maturity Implication	**No direct alignment.** LastPass does not provide patch deployment, verification or reporting capability. Vault access continuity supports operational recovery but does not contribute to Maturity Level One requirements.
Client Responsibility	Use patch management tools to maintain application currency.

2. Patch Operating Systems (OS)

Objective: Patch OS vulnerabilities

Relevant ISM Controls: ISM-0304, ISM-1695

Assessment:

Direct Support	Not provided. OS patching is out of scope.
Indirect Benefit	Cloud-based credential access is available after OS rebuild, supporting recovery.
Maturity Implication	**No direct alignment.** LastPass does not contribute to operating system patch management. Access to vault data after reimaging may aid incident recovery but does not influence OS patching maturity.
Client Responsibility	Implement and monitor OS patching using dedicated tools.

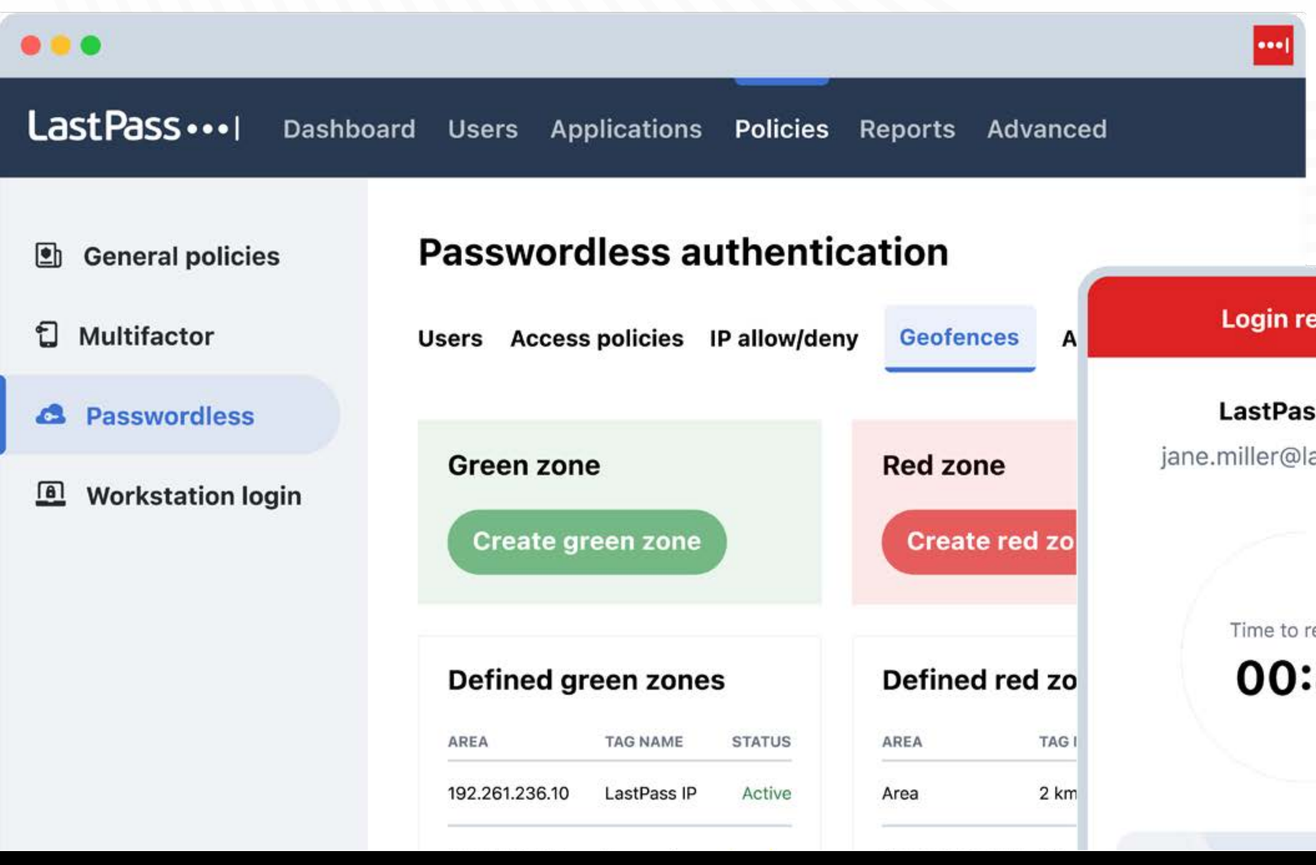
3. Multi-Factor Authentication (MFA)

Objective: Enforce MFA for remote, privileged, and sensitive access

Relevant ISM Controls: ISM-1504, ISM-1872

Assessment:

Direct Support	Native MFA (TOTP, push, FIDO2), IdP integration, and policy enforcement for vault and admin access. FIDO2 and biometrics options meet the highest assurance expectations.
Maturity Implication	**Supports Maturity Level Three.**
Client Responsibility	Enforce MFA policies across all users and integrate with SIEM.



4. Restrict Administrative Privileges

Objective: Control and monitor use of administrative privileges

Relevant ISM Controls: ISM-1507, ISM-1509, ISM-1815

Assessment:

Direct Support	Centralised RBAC, delegated admin, audit logging, and privileged credential sharing.
Indirect Benefit	Supports linking privileged access to IdP policies and logs. Just-in-Time Access (JIT) is not available and must be managed via existing delegation and approval workflows.
Maturity Implication	**Supports ACSC Maturity Level Two.** Maturity Level 3 outcomes — such as JIT access, isolated admin environments, and session credential isolation — require integration with dedicated Privileged Access Management (PAM) and Endpoint Detection Response (EDR) tools.
Client Responsibility	Maintain oversight of admin access and integrate with broader privileged access management processes.

5. Application Control

Objective: Prevent unauthorised applications from executing

Relevant ISM Controls: ISM-0296, ISM-0300

Assessment:

Direct Support	Not provided. LastPass does not offer allowlisting or execution control.
Indirect Benefit	Restricts credential autofill to authorised/verified domains, reducing the risk of credential leakage to malicious or unauthorised apps. Works alongside traditional application control tools by limiting where credentials can be entered.
Maturity Implication	**No direct alignment.** Domain-based autofill reduces credential leakage but is not a substitute for application execution controls.
Client Responsibility	Implement application allowlisting and endpoint controls.

6. Configure Microsoft Office Macros

Objective: Prevent untrusted macros from executing

Relevant ISM Controls: ISM-1579, ISM-1863

Assessment:

Direct Support	Not provided. LastPass does not manage macros or Microsoft Office policies.
Indirect Benefit	Secure vault storage discourages password reuse and storage in Microsoft Office files, lowering the impact of macro-based attacks aimed at harvesting credentials.
Maturity Implication	**No direct alignment.** No contribution to macro control maturity. Credential hygiene is improved, but macro configuration and enforcement must be managed through Microsoft policies and endpoint controls.
Client Responsibility	Configure and enforce macro policies via endpoint management.

7. User Application Hardening

Objective: Harden applications to reduce attack surface

Relevant ISM Controls: ISM-1859, ISM-1860

Assessment:

Direct Support	Not provided. LastPass does not harden applications.
Indirect Benefit	Browser extension restricts autofill to verified domains, reducing risk of credential theft via spoofed or compromised sites. Avoids storing passwords insecurely within applications. Supports credential discipline and reduces misuse risk.
Maturity Implication	Supports **ACSC Maturity Level One** when the browser extension is deployed and managed using enterprise MDM or group policy controls.
Client Responsibility	Maintain enterprise-wide backup for all systems and data.

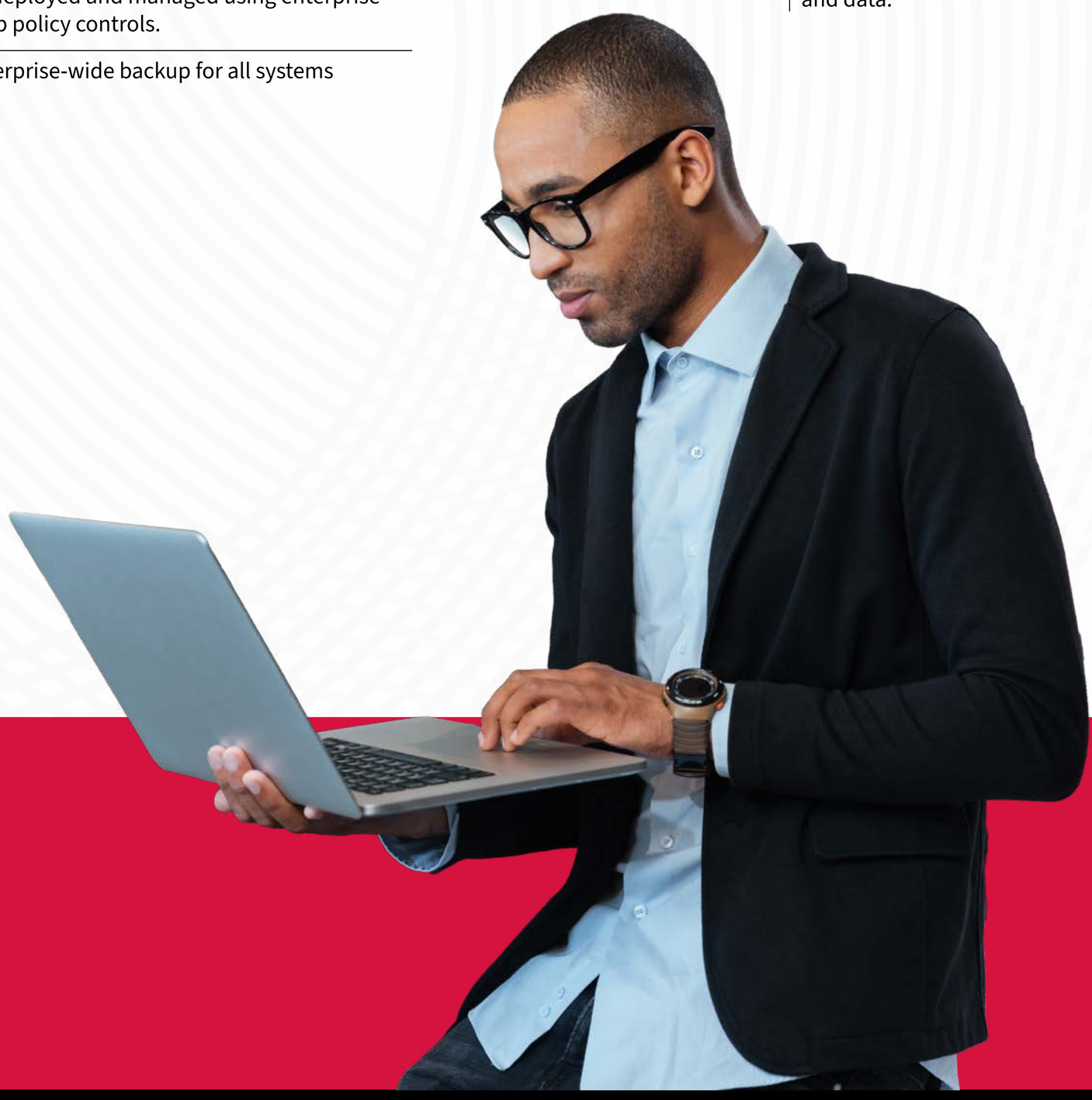
8. Regular Backups

Objective: Back up and securely store critical data

Relevant ISM Controls: ISM-0343, ISM-0344

Assessment:

Direct Support	Not provided. Does not back up client endpoints or files.
Indirect Benefit	LastPass performs encrypted, redundant backups for vault data, ensuring credential recoverability.
Maturity Implication	**No direct alignment.** Vault redundancy ensures credential availability, but enterprise data backups must meet Australian Cyber Security Centre (ACSC) requirements independently.
Client Responsibility	Maintain enterprise-wide backup for all systems and data.



Summary Table

Essential Eight Strategy	What LastPass Delivers	Example Benefit for Organisation	What Clients Still Need to Do
1. Patch Applications	Secure vault for fast operational recovery	Credentials are available after patching incidents	Use patch management tools to maintain application currency
2. Patch Operating Systems	Vault stays accessible after OS rebuild	Users regain access quickly post-incident	Implement and monitor OS patching using dedicated tools
3. **Multi-Factor Authentication (Level 3)**	MFA (FIDO2, biometrics, SSO, policy enforcement)	Stops credential attacks even if passwords stolen	Enforce MFA policies across all users and integrate with SIEM
4. **Restrict Admin Privileges (Level 2)**	RBAC, admin delegation, full audit logging	Prevents shared/generic admin accounts; full audit trail	Maintain oversight of admin access and integrate with broader privileged access management processes
5. Application Control	Autofill only on trusted web domains	Prevents users from entering credentials in risky apps	Implement application allow listing and endpoint controls
6. Configure Office Macros	Discourages storing passwords in Office files	Reduces the risk of password theft via macro attacks	Configure and enforce macro policies via endpoint management
7. **User App Hardening (Level 1 w/ browser extension)**	Strong password enforcement; browser extension	Stops weak/reused passwords in web applications	Harden browsers, PDF readers, and other user apps
8. Regular Backups	Encrypted, redundant vault backups	Credential data recoverable after ransomware/disaster	Maintain enterprise-wide backup for all systems and data.

LastPass strongly aligns with Essential Eight identity-focused strategies, particularly **Multi-Factor Authentication (Level Three)** and **Restricting Administrative Privileges (Level Two)**. Indirect benefits exist across other domains, enhancing credential hygiene and continuity.

For full cyber maturity, LastPass should be integrated with complementary solutions for patching, application control, macros, and backup. Achieving higher maturity levels will depend on broader integration with SIEM, Endpoint Detection Response (EDR), Mobile Device Management (MDM), and Privileged Access Management (PAM) platforms.

Contact LastPass today