Strategic Compliance Report (Essential Eight Maturity Assessment)

This document is a simplified version for technical portfolio demonstration purposes, focusing on strategic structure and alignment with COBIT, ISO, or ITIL frameworks.

Aligned with ACSC Essential Eight Maturity Model

ACSC Australian Cyber Security Centre

Introduction

This report assesses the maturity of cybersecurity controls at CloudNova Logistics' Australian subsidiary, using the eight essential mitigation strategies recommended by the Australian Cyber Security Centre (ACSC).

Maturity Level Summary

Our current goal is to achieve Maturity Level 2 (protection against adversaries who use known and effective intrusion tools and techniques).

Strategy Evaluation

MITIGATION TO PREVENT ATTACKS

Application Control: Partially implemented. Known software is allowed, but there is still no total blocking of executables in user profile folders. (Status: Level 1).

Patch Applications: Automated process for browsers and Office. Critical vulnerabilities are fixed within 48 hours. (Status: Level 3).

Microsoft Office Macro Settings: Macros disabled globally for files originating from the internet via GPO. (Status: Level 3).

User Application Hardening: Blocking of Flash and unauthorized browser extensions. (Status: Level 2).

Strategy Evaluation

MITIGATION TO LIMIT IMPACT

Restrict Administrative Privileges: Admin accounts reviewed. Regular users don't have local privileges. (Status: Level 3).

Patch Operating Systems: Monthly update of servers and workstations. Gap identified in legacy servers. (Status: Level 2).

Multi-Factor Authentication (MFA): Implemented for all remote access (VPN) and administrative privilege accounts. (Status: Level 3).

Strategy Evaluation

MITIGATION TO AVAILABILITY

- **Regular Backups:** Daily backups performed with 3 months of retention.
    - **Area for Improvement:** Implement “Immutable” storage (offline/protected cloud) to ensure total protection against ransomware. (Status: Level 2).

Action Plan (Remediation Roadmap)

PRIORITY 1

Elevate Application Control to Level 2, implementing execution blocking in temporary directories (%appdata%).

PRORITY 2

Modernize legacy servers to ensure that 100% of the operational fleet can receive security patches.

Conclusion

CloudNova Logistics Australia has a solid security foundation, operating at an average maturity of Level 2. The immediate focus on Application Control will dramatically reduce the risk of modern malware execution.

Disclaimer

This document represents a fictional case developed for professional and educational purposes and does not reflect any real organization.