Microsoft Office Macro Settings (Essential Eight)

1. Mitigation Strategy Overview

Name: Configure Microsoft Office Macro Settings
Essential Eight Category: Mitigation Strategy
Objective:

- Prevent malicious macros from running in Microsoft Office applications (Word, Excel, PowerPoint).
- Ensure that only approved users can run macros, and macros from the internet or email are automatically blocked.

Macros are often exploited by attackers to deliver malware, making this an important baseline security measure.

2. Maturity Level 1 Controls

The ASD Essential Eight defines the following controls for ML1:

Test ID	Control Requirement	What It Means
ML1-OM-01	Block macros for unapproved users	Non-approved users must not be able to run macros.
ML1-OM-02	Maintain approved macro user list	There must be a documented list of users allowed to run macros.
ML1-OM-03	Block macros from the internet	Office files downloaded from email or web must have macros blocked.
ML1-OM-04	Enforce GPO & registry settings	Registry key blockcontentexecutionfromInternet must be set to 1.
ML1-OM-05	Enable macro antivirus scanning	Macros must be scanned by antivirus before execution.
ML1-OM-06	Detect malicious macros	Antivirus must detect known malicious macros (test with EICAR).
ML1-OM-07	Prevent users from changing settings	Standard users must not be able to enable macros on their own.

3. Why It's Important for the Evidence Collector

- **Automation Potential:** Macro settings can be verified using PowerShell or registry checks.
- **Clear Evidence Points:** Screenshots of Group Policy, registry keys, and blocked macro alerts are straightforward evidence.
- **Compliance Alignment:** Fully aligns with ASD Essential Eight and APRA CPS 234's malware prevention requirements.

4. How Evidence Collector & Validator Will Work

1. **Group Policy Reports:**
    - Run gpresult /h report.html and parse the section for Microsoft Office Macro Settings.
2. **File Behavior Test:**
    - Open a .docm file downloaded from the internet.
    - Capture the **"Macros have been disabled"** banner.
3. **User Access Test:**
    - Check if standard users can change macro settings in **Trust Center**

4.2 Evidence Validation

- Compare registry and GPO results against the expected values (e.g., blockcontentexecutionfromInternet must be 1).
- Verify test file execution behavior matches policy (macro blocked).

5. Example Evidence Outputs

Your tool or manual validation could produce:

Screenshot Examples:

- **Group Policy:** Macro settings disabled.
- **Registry:** blockcontentexecutionfromInternet = 1.
- **Blocked Macro Banner:** Office warning message.
- **Trust Center (Greyed Out):** User cannot modify settings.

Sample JSON Output:

{

"test_id": "ML1-OM-03",

"description": "Macros from internet are blocked",

"registry": "blockcontentexecutionfromInternet = 1",

"file_test": "macro_blocked_banner_displayed",

"result": "PASS"

}

6. Mapping to Policy Frameworks

Framework	Mapping
ASD Essential Eight	Strategy 3: Configure Microsoft Office Macro Settings
APRA CPS 234	Sections 20(a), 21(a): Security controls must mitigate malware and unauthorized code execution.

7. Example Websites for Testing

- **EICAR Test File:** https://www.eicar.org (for safe AV testing).
- **Office Macro Test Files:** Create .docm or .xlsm files locally with a simple macro, or download test files from trusted security research sites.

8. Next Steps for Your Team

1. **Create/Download macro test files** (safe .docm).
2. **Capture screenshots** of:
    - Group Policy macro setting.
    - Registry key (blockcontentexecutionfromInternet).
    - Blocked macro banner.
    - Trust Center (showing user cannot change).
3. **Document results** in your Evidence Collector structure (JSON/Excel).
4. **Validate and map** findings to ML1 controls.

9. Integration with Evidence Collector & Validator (EC&V)

To ensure our Microsoft Office Macro Settings mapping integrates seamlessly with the team's broader Evidence Collector & Validator (EC&V) platform, the following technical enhancements and architecture considerations are incorporated:

Evidence Integrity and Tamper Detection

To ensure the authenticity and integrity of submitted evidence:

- A **SHA-256 hash** is generated for each uploaded screenshot.
- The system stores metadata including:
    - Uploader email or username
    - Timestamp of submission
    - Test ID mapped
    - Hash value for file integrity

Example JSON structure:


```
{
 "test_id": "ML1-OM-03",
 "description": "Macros from internet are blocked",
 "file": "macro_banner.png",
 "hash": "c61e750274842da3f38eaf9e2bf57a10e2131ecf41f13534a25629f58b84bfc3",
 "uploaded_by": "analyst1@company.com",
 "timestamp": "2025-08-03T15:30:00",
 "status": "LOCKED"
}
```


This allows the tool to verify whether evidence has been altered or replaced after submission.

Optical Character Recognition (OCR) and NLP Support

To reduce manual review burden, the EC&V system uses:

- **OCR** to extract visible text from screenshots (e.g., Group Policy settings, Registry values).
- **Natural Language Processing (NLP)** to:
    - Identify relevant control keywords (e.g., “disable macros”, “block internet macros”).
    - Match extracted phrases against known Essential Eight control descriptions.

This enables **automatic matching** of screenshots to corresponding ML1 requirements even without structured config files.

Evidence Validation Rules

The EC&V applies the following logic to ensure high-quality, audit-ready evidence:

Validation Check	Logic Description
Registry Match	Confirms blockcontentexecutionfromInternet = 1
Macro Banner Detection	Confirms presence of "Macros have been disabled" banner in Office UI
Access Lock Test	Verifies Trust Center settings are non-editable by standard users
Blurred or Incomplete Screenshot	If OCR detects unreadable or partial content, evidence is flagged as invalid
Duplicate Submission	Same hash = flagged to avoid duplicate or reused screenshots

Upload Control and Audit Logging

To support secure operations:

- **Upload access** is restricted to authorized cybersecurity/IT staff.
- All actions (upload, delete, update) are tracked with:
    - Username
    - Timestamp
    - IP address (optional)
    - Affected test ID
- Once submitted, **evidence is locked** to prevent changes, unless re-opened by an authorized auditor or admin.
- Locked files display a visual badge: Evidence Locked

Policy Mapping and Reporting

- Mapped results from the macro validation (e.g., PASS/FAIL status, associated hash, extracted text) feed directly into the **auto-generated audit reports**.

- These reports align with:
    - **ASD Essential Eight**: Strategy 3
    - **APRA CPS 234**: Sections 20(a), 21(a)
- Final reports can be exported in Excel or JSON for external audit submission or internal review.

Summary of Enhancements

Feature	Benefit
SHA-256 Hashing	Detects tampering or duplicate uploads
OCR + NLP Integration	Automates text extraction from screenshots for validation
Blurred/Incomplete Detection	Improves reliability of submitted evidence
Role-Based Access & Locking	Ensures only authorized personnel upload and edit sensitive audit artifacts
Direct Framework Mapping	Ensures full traceability from evidence to ASD/APRA control points