CMMC 2.0 Compliance Roadmap

CONTENTS

CMMC 2.0 Compliance Roadmap - mail.stsgym.com

Generated: 2026-03-08 **Current Status:** Level 1: ~60% | Level 2: ~30%
Target: Level 1: 100% | Level 2: 80%+

Executive Summary

This document outlines the steps required to achieve CMMC 2.0 Level 1 and Level 2 compliance for mail.stsgym.com. CMMC (Cybersecurity Maturity Model Certification) is required for organizations handling Controlled Unclassified Information (CUI) or working with the Department of Defense.

Current Gaps

Category	Level 1 Gap	Level 2 Gap
Access Control	Root SSH enabled	No MFA
Audit Logging	No auditd	No SIEM
Authentication	Password policy weak	No MFA

Category	Level 1 Gap	Level 2 Gap
Incident Response	No formal plan	No formal plan
Configuration	Partial hardening	No CM
Vulnerability Mgmt	No scanning	No continuous

CMMC 2.0 Level 1 Compliance (17 Practices)

AC.L1-3.1.001 - Access Control Policy

Requirement: Limit information system access to authorized users.

Current State: ⚠ Partial - Root SSH was enabled (now fixed)

Actions Required: 1. ✅ Disable root SSH login (COMPLETED via script) 2. Document access control policy 3. Implement role-based access (RBAC) 4. Review user access quarterly

Commands:

```
# Verify root SSH disabled
grep "^PermitRootLogin" /etc/ssh/sshd_config

# List all users with shell access
grep -E '/bin/bash|/bin/sh' /etc/passwd

# Review sudo users
cat /etc/sudoers | grep -v '^#' | grep -v '^$'
```

AC.L1-3.1.002 - Account Management

Requirement: Establish accounts for authorized users.

Current State: ✅ Pass - Users defined

Actions Required: 1. Create account management procedure 2. Document account creation/approval workflow 3. Implement account termination process 4. Maintain user access roster

Documentation Needed: - Account request form - Access approval workflow - Termination checklist - Quarterly access review record

---

AC.L1-3.1.003 - Access Enforcement

Requirement: Enforce approved authorizations.

Current State: ⚠ Partial - Need RBAC

Actions Required: 1. Create user groups for different access levels 2. Implement sudo rules for privileged commands 3. Document access rights by role 4. Configure file permissions

Commands:

```
        # Create groups
        sudo groupadd web-admin
        sudo groupadd db-admin
        sudo groupadd mail-admin

        # Add users to groups
        sudo usermod -aG web-admin wez
        sudo usermod -aG db-admin wez

        # Create sudo rules file
        sudo cat > /etc/sudoers.d/roles << 'EOF'
        # Web administrators - can manage nginx and web service
        %web-admin ALL=(ALL) /usr/bin/systemctl restart nginx
        %web-admin ALL=(ALL) /usr/bin/systemctl restart stsgym-
website
        %web-admin ALL=(ALL) /usr/bin/docker restart *

        # Database administrators - can manage postgres/redis
        %db-admin ALL=(ALL) /usr/bin/docker exec * psql *
        %db-admin ALL=(ALL) /usr/bin/systemctl restart postgres

        # Full admin - wez
        wez ALL=(ALL) ALL
        EOF

        # Verify syntax
        sudo visudo -c
```

AU.L1-3.3.001 - Audit Events

Requirement: Create audit log records.

Current State: ❌ Fail - No auditd (being fixed by script)

Actions Required: 1. □ Install and configure auditd (COMPLETED via script) 2. Configure audit rules for security events 3. Ensure logs are written to persistent storage 4. Test audit logging

Commands:

```
# Verify auditd running
sudo systemctl status auditd

# List audit rules
sudo auditctl -l

# Search audit logs
sudo ausearch -ts today -m USER_LOGIN

# Generate audit report
sudo aureport --summary
```

Audit Rules Configured: - User/group changes - Privilege escalation - Login attempts - File modifications - Network configuration changes

---

AU.L1-3.3.002 - Audit Content

Requirement: Ensure audit records contain required information.

Current State: □ Pass - auth.log exists

Actions Required: 1. Verify log format includes timestamp, user, action 2. Configure rsyslog for centralized logging 3. Ensure sufficient log retention (90+ days)

Commands:

```
# Check auth log format
sudo tail -5 /var/log/auth.log

# Configure log retention
sudo cat >> /etc/logrotate.conf << 'EOF'
/var/log/auth.log {
    weekly
    rotate 13
    compress
    delaycompress
```

```
        missingok
        notifempty
        create 0640 syslog adm
    }
    EOF
```

AU.L1-3.3.003 - Protect Audit Information

Requirement: Protect audit information from unauthorized access.

Current State: □ Pass - Logs restricted

Actions Required: 1. Verify log permissions 2. Restrict root-only access to sensitive logs 3. Configure log integrity checking

Commands:

```
    # Check log permissions
    ls -la /var/log/auth.log /var/log/syslog

    # Should show: -rw-r----- 1 syslog adm
    # If not, fix:
    sudo chmod 0640 /var/log/auth.log
    sudo chown syslog:adm /var/log/auth.log
```

CA.L1-3.5.001 - Authentication for Organizational Systems

Requirement: Authenticate access to organizational systems.

Current State: ⚠ Partial - SSH keys OK, but password also allowed

Actions Required: 1. Verify password authentication disabled for SSH 2. Document authentication methods 3. Implement SSH key management

Commands:

```
    # Check SSH auth methods
    grep -E "PasswordAuthentication|PubkeyAuthentication" /
ssh/sshd_config.d/*.conf

    # Should show: PasswordAuthentication no
    # If not, create override:
```

```
sudo cat > /etc/ssh/sshd_config.d/99-hardening.conf <<
PasswordAuthentication no
PubkeyAuthentication yes
PermitRootLogin no
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 2
EOF

sudo systemctl restart ssh
```

CA.L1-3.5.002 - Password Policy

Requirement: Enforce password complexity and expiration.

Current State: □ Fail - Passwords never expire (being fixed)

Actions Required: 1. □ Set PASS_MAX_DAYS to 90 (COMPLETED) 2. Configure password complexity 3. Implement password history

Commands:

```
# Verify password policy
grep -E "PASS_MAX|PASS_MIN|PASS_WARN" /etc/login.defs

# Should show:
# PASS_MAX_DAYS   90
# PASS_MIN_DAYS   0
# PASS_WARN_AGE   7

# Install password quality module
sudo apt install -y libpam-pwquality

# Configure complexity
sudo cat >> /etc/security/pwquality.conf << 'EOF'
minlen = 14
minclass = 4
maxrepeat = 2
maxsequence = 3
```

```
difok = 4
EOF
```

IA.L1-3.5.001 - Identify Users

Requirement: Identify users and processes.

Current State: □ Pass - Accounts defined

Actions Required: 1. Maintain user inventory 2. Document user roles 3. Link users to individuals

---

IA.L1-3.5.002 - Authentication Mechanisms

Requirement: Use authentication mechanisms for access.

Current State: ⚠ Partial - SSH keys + password

Actions Required: 1. Document authentication methods 2. Configure password policy 3. Consider hardware tokens for privileged access

---

IA.L1-3.5.003 - Multi-Factor Authentication

Requirement: Implement MFA for privileged access.

Current State: □ Fail - No MFA

Actions Required: 1. Install Google Authenticator PAM module 2. Configure for SSH 3. Enroll users 4. Document MFA procedure

Commands:

```
# Install MFA
sudo apt install -y libpam-google-authenticator

# Configure for SSH
sudo sed -i 's/^@include common-auth/@include common-
auth\nauth required pam_google_authenticator.so/' /etc/pam.d/
sshd

# Configure SSH to use MFA
sudo sed -i 's/^UsePAM yes/UsePAM yes\nAuthenticationMe
publickey,keyboard-interaction/' /etc/ssh/sshd_config
```

```
sudo systemctl restart ssh

# For each user:
google-authenticator
```

IR.L1-3.6.001 - Incident Response Plan

Requirement: Establish incident response capability.

Current State: ⚠ Partial - fail2ban active but no formal plan

Actions Required: 1. Create incident response plan 2. Define incident types 3. Document response procedures 4. Assign roles and responsibilities

Template:

```
# Incident Response Plan

## Incident Types
1. Unauthorized access attempt
2. Malware detection
3. Data breach
4. Denial of service
5. Configuration change

## Response Procedures

### Unauthorized Access
1. Isolate affected account
2. Review audit logs
3. Block IP via fail2ban/UFW
4. Notify administrator
5. Document incident

### Malware Detection
1. Isolate affected system
2. Run ClamAV scan
3. Quarantine affected files
4. Review process list
5. Document and report
```

```
## Contact Information
- Primary: [Admin Name]
- Backup: [Backup Contact]
- Security: [Security Team]
```

MA.L1-3.7.001 - Maintenance

Requirement: Perform maintenance on organizational systems.

Current State: ⚠ Partial - Unattended upgrades enabled

Actions Required: 1. Document maintenance schedule 2. Schedule regular updates 3. Document backup procedures 4. Test recovery procedures

---

MP.L1-3.8.001 - Media Protection

Requirement: Protect media containing CUI.

Current State: ⚠ N/A - Cloud VPS

Actions Required: 1. Document backup procedures 2. Verify encryption at rest (check with provider) 3. Implement backup verification

Commands:

```
# Set up automated backups
sudo apt install -y rsnapshot

# Configure backup retention
sudo cat > /etc/rsnapshot.conf << 'EOF'
config_version  1.2
snapshot_root   /backup/
no_create_root   1

cmd_cp          /bin/cp
cmd_rm          /bin/rm
cmd_rsync       /usr/bin/rsync
cmd_ssh /usr/bin/ssh
cmd_logger      /usr/bin/logger
cmd_du          /usr/bin/du
cmd_rsnapshot_diff      /usr/bin/rsnapshot-diff
cmd_preexec     /path/to/preexec/script
```

```
        cmd_postexec    /path/to/postexec/script

        retain  daily   7
        retain  weekly  4
        retain  monthly 3

        backup  /home/           localhost/
        backup  /etc/           localhost/
        backup  /var/log/       localhost/
        EOF
```

PE.L1-3.10.001 - Physical Access

Current State: ⚠ N/A - Cloud VPS

Actions Required: 1. Document that server is cloud-hosted 2. Note provider's physical security controls 3. Maintain inventory of physical assets

---

SC.L1-3.13.001 - System and Communications Protection

Requirement: Protect systems from unauthorized access.

Current State: ⚠ Partial - TLS OK, gaps exist

Actions Required: 1. ☐ Verify TLS configuration (done) 2. Review and harden all services 3. Implement network segmentation

---

SC.L1-3.13.002 - Boundary Protection

Requirement: Protect system boundaries.

Current State: ☐ Pass - UFW active

Actions Required: 1. Document firewall rules 2. Review open ports quarterly 3. Implement change control for firewall changes

---

SI.L1-3.14.001 - Malicious Code Protection

Requirement: Implement malicious code protection.

Current State: ☐ Fail - No AV (being installed by script)

Actions Required: 1. ☐ Install ClamAV (COMPLETED via script) 2. Configure daily scans 3. Document scan results

Commands:

```
        # Update ClamAV signatures
        sudo freshclam

        # Schedule daily scan
        sudo cat > /etc/cron.daily/clamscan << 'EOF'
        #!/bin/bash
        /usr/bin/clamscan -r /home /etc /var/www --quiet --log
log/clamav/daily.log
        if [ $? -eq 1 ]; then
            mail -s "ClamAV: Malware Detected" root@localhost <
log/clamav/daily.log
        fi
        EOF
        sudo chmod +x /etc/cron.daily/clamscan
```

SI.L1-3.14.002 - Monitoring and Detection

Requirement: Monitor for security events.

Current State: ⚠ Partial - Logs exist, no monitoring

Actions Required: 1. Configure log monitoring 2. Set up alerts for security events 3. Review logs daily

Commands:

```
        # Install logwatch for daily reports
        sudo apt install -y logwatch

        # Configure daily email
        sudo cat > /etc/cron.daily/logwatch-report << 'EOF'
        #!/bin/bash
        /usr/sbin/logwatch --output mail --mailto root@localhos
        EOF
        sudo chmod +x /etc/cron.daily/logwatch-report
```

SI.L1-3.14.003 - Spam Protection

Requirement: Implement spam protection.

Current State: ✅ Pass - Postfix configured with TLS

Actions Required: 1. Document spam protection measures 2. Configure SpamAssassin if not already

Commands:

```
        # Install SpamAssassin
        sudo apt install -y spamassassin spamc

        # Configure Postfix
        sudo postconf -e 'content_filter = spamassassin'
        sudo postconf -e 'spamassassin_destination_recipient_li
1'

        # Create spamassassin service
        sudo cat > /etc/postfix/master.cf.d/spamassassin.cf <<
        spamassassin unix - n n - - pipe
          user=debian-spamd argv=/usr/bin/spamc -f -e /usr/sbin/
sendmail -oi -f ${sender} ${recipient}
        EOF
```

CMMC 2.0 Level 2 Compliance (110+ Practices)

Level 2 adds 93+ practices beyond Level 1. Here are the key additions needed:

Access Control (AC)

Practice	Requirement	Current	Action Needed
AC.L2-3.1.007	Network access control	⚠ Partial	Implement network segmentation
AC.L2-3.1.008	System boundary protection	⚠ Partial	Document all network boundaries
AC.L2-3.1.009	Transmission security	✅ Pass	TLS already implemented
AC.L2-3.1.013	Mobile device policy	❌ Fail	Create mobile device policy

Practice	Requirement	Current	Action Needed
AC.L2-3.1.014	Wireless access control	❌ Fail	Document wireless policy

Audit (AU)

Practice	Requirement	Current	Action Needed
AU.L2-3.3.004	Audit review	❌ Fail	Schedule weekly log reviews
AU.L2-3.3.005	Correlation	❌ Fail	Implement SIEM
AU.L2-3.3.006	Retention	⚠ Partial	Extend log retention to 1 year
AU.L2-3.3.007	Protection	✅ Pass	Logs protected

Configuration Management (CM)

Practice	Requirement	Current	Action Needed
CM.L2-3.4.001	Baseline configuration	❌ Fail	Document baseline
CM.L2-3.4.002	Change control	❌ Fail	Implement change control
CM.L2-3.4.003	Authorized changes	❌ Fail	Document change approval
CM.L2-3.4.004	Configuration monitoring	❌ Fail	Implement config monitoring

Identification & Authentication (IA)

Practice	Requirement	Current	Action Needed
IA.L2-3.5.004	Unique identification	✅ Pass	Users have unique IDs
IA.L2-3.5.005	Authenticator management	❌ Fail	Document key management
IA.L2-3.5.006	Authenticator feedback	⚠ Partial	Configure password feedback
IA.L2-3.5.007	Cryptographic protection	⚠ Partial	Document key storage

Incident Response (IR)

Practice	Requirement	Current	Action Needed
IR.L2-3.6.002	Incident response training	❌ Fail	Conduct IR training
IR.L2-3.6.003	Incident testing	❌ Fail	Test IR procedures
IR.L2-3.6.004	Incident handling	❌ Fail	Document procedures

Maintenance (MA)

Practice	Requirement	Current	Action Needed
MA.L2-3.7.003	Maintenance tools	⚠ Partial	Document all tools
MA.L2-3.7.004	Maintenance personnel	⚠ Partial	Document personnel
MA.L2-3.7.005	Maintenance records	❌ Fail	Keep maintenance logs

Media Protection (MP)

Practice	Requirement	Current	Action Needed
MP.L2-3.8.002	Media access	⚠ N/A	Cloud-hosted
MP.L2-3.8.003	Media marking	⚠ N/A	Cloud-hosted
MP.L2-3.8.004	Media storage	⚠ N/A	Cloud-hosted

Personnel Security (PS)

Practice	Requirement	Current	Action Needed
PS.L2-3.11.002	Personnel screening	❌ Fail	Document screening policy
PS.L2-3.11.003	Personnel termination	❌ Fail	Document termination process

System and Communications Protection (SC)

Practice	Requirement	Current	Action Needed
SC.L2-3.13.003	Separation of duties	⚠ Partial	Document role separation
SC.L2-3.13.004	Session lock	❌ Fail	Configure session timeout
SC.L2-3.13.005	Boundary protection	✅ Pass	UFW configured

System Integrity (SI)

Practice	Requirement	Current	Action Needed
SI.L2-3.14.004	Vulnerability scanning	❌ Fail	Install vulnerability scanner
SI.L2-3.14.005	Malicious code protection	⚠ Partial	ClamAV installed
SI.L2-3.14.006	Update management	✅ Pass	Unattended upgrades

Implementation Timeline

Phase 1: Immediate (Week 1)

Task	Status	Responsible
Disable root SSH login	✅ Done	Script
Enable auditd	✅ Done	Script
Set password expiration	⚠ Needs verification	Admin
Install ClamAV	✅ Done	Script
Apply kernel hardening	✅ Done	Script

Phase 2: Short-term (Weeks 2-4)

Task	Priority	Effort
Configure PostgreSQL password	HIGH	1 hour
Configure Redis password	HIGH	30 min
Implement MFA for SSH	HIGH	2 hours
Create incident response plan	MEDIUM	4 hours
Configure log monitoring	MEDIUM	2 hours
Document access control policy	MEDIUM	2 hours

Phase 3: Medium-term (Months 1-3)

Task	Priority	Effort
Implement RBAC	MEDIUM	8 hours
Set up vulnerability scanning	MEDIUM	4 hours
Configure centralized logging	MEDIUM	4 hours
Create configuration baseline	MEDIUM	4 hours
Implement change control	MEDIUM	4 hours
Document all procedures	MEDIUM	8 hours

Phase 4: Long-term (Months 3-6)

Task	Priority	Effort
Implement SIEM	LOW	16 hours
Conduct security training	LOW	4 hours
Test incident response	LOW	4 hours
Third-party security assessment	LOW	8 hours
CMMC certification prep	LOW	40 hours

Quick Reference Commands

Verify Current Status

```
        # Check SSH configuration
        grep -E "PermitRootLogin|PasswordAuthentication" /etc/s
sshd_config*

        # Check audit status
        sudo systemctl status auditd
        sudo auditctl -l

        # Check password policy
        grep -E "PASS_MAX|PASS_MIN|PASS_WARN" /etc/login.defs

        # Check ClamAV
        clamscan --version
        sudo systemctl status clamav-daemon

        # Check firewall
        sudo ufw status verbose

        # Check fail2ban
        sudo fail2ban-client status sshd

        # Check open ports
        ss -ltnup

        # Check user accounts
        grep -E '/bin/bash|/bin/sh' /etc/passwd

        # Check audit logs
        sudo aureport --summary
```

Security Hardening Script

```
        # Run on the server
        wget https://raw.githubusercontent.com/.../security-
hardening-mail.sh
```

```
chmod +x security-hardening-mail.sh
sudo ./security-hardening-mail.sh
```

Documentation Templates

Access Control Policy Template

```
# Access Control Policy

## Purpose
Define requirements for controlling access to organizat
systems.

## Scope
Applies to all users of mail.stsgym.com and related ser

## Policy Statements
1. Access shall be granted based on least privilege
2. All access requests require approval from system
administrator
3. Access shall be reviewed quarterly
4. Inactive accounts shall be disabled after 90 days
5. Privileged access requires additional authentication

## Roles and Responsibilities
- System Administrator: Approve and manage accounts
- Users: Protect credentials, report incidents
- Management: Approve policy changes

## Enforcement
Violations may result in access revocation and discipli
action.
```

Incident Response Plan Template

```
# Incident Response Plan

## Incident Types
```

```
        1.
**Unauthorized Access**: Attempted or successful access by
unauthorized user
        2. **Malware**: Detection of malicious software
        3. **Data Breach**: Unauthorized access to sensitive da
        4. **Denial of Service**: Disruption of service availab
        5. **Configuration Change**: Unauthorized modification
system configuration

        ## Response Procedures

        ### Unauthorized Access
        1. Isolate affected account: `sudo usermod -L <username
        2. Block IP: `sudo ufw deny from <IP>`
        3. Review logs: `sudo journalctl -u sshd --since "1 hou
ago"`
        4. Document incident in security log
        5. Notify administrator

        ### Malware Detection
        1. Isolate system: Disconnect from network if severe
        2. Run scan: `sudo clamscan -r /`
        3. Quarantine files: `sudo mv <file> /quarantine/`
        4. Document findings
        5. Report to administrator

        ### Data Breach
        1. Identify scope: Review audit logs
        2. Preserve evidence: Do not modify logs
        3. Contain: Revoke compromised credentials
        4. Document: Record all findings
        5. Notify: Report to affected parties

        ## Contact Information
        - Primary Administrator: [Name, Email, Phone]
        - Backup Administrator: [Name, Email, Phone]
        - Security Team: [Contact]
```

Next Steps

1. **Run the security hardening script** on the server
2. **Document all policies** using the templates above
3. **Configure PostgreSQL and Redis passwords**
4. **Implement MFA** for SSH access
5. **Schedule quarterly reviews** of this compliance plan

Last Updated: 2026-03-08 Next Review: 2026-04-08