Assignment 3 - CCI and Incident Response
CCI Implementation Plan
CSE 4380

Group Thorin

April 11th, 2025

Members:	Obadah Al-Smadi
	Betim Hodza
	Elliot Mai
	Benjamin Niccum
	Nicholas Pratt
Instructor:	Trevor Bakker

Contents

1 Access Control (AC) CCIs

1.1 Detailed Specifications

The Access Control family includes the following key controls that must be implemented for the AeroTech X9 drone system:

- **AC-1 (Policy and Procedures)**: Requires developing, documenting, and disseminating access control policies that address purpose, scope, roles, and responsibilities.
- **AC-2 (Account Management)**: Requires identifying and selecting system accounts that support organizational missions and business functions.
- **AC-3 (Access Enforcement)**: Requires enforcing approved authorizations for logical access to information and system resources.
- **AC-6 (Least Privilege)**: Employs the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned tasks.
- **AC-17(7) (Remote Access — Additional Protection for Security Function Access)**: Implements additional protection for remote access to security functions.
- **AC-18 (Wireless Access)**: Establishes usage restrictions, configuration requirements, and implementation guidance for wireless access.
- **AC-18(2) (Wireless Access — Monitoring Unauthorized Connections)**: Monitors for unauthorized wireless connections to the information system.
- **AC-19 (Access Control for Mobile Devices)**: Establishes usage restrictions, configuration requirements, and implementation guidance for mobile devices.

1.2 Technical Configurations and Procedural Requirements

To implement these controls for the AeroTech X9 drone system, the following technical configurations and procedures must be established:

1. **Access Control Policies**:
   - Document comprehensive access control policies at organizational, mission, and system levels
   - Implement review procedures to ensure policies are updated at least annually
   - Establish formal approval processes for policy changes
2. **Account Management System**:
   - Deploy automated account management tools to handle account creation, modification, and termination
   - Configure role-based access controls aligned with separation of duties requirements
   - Implement automatic disabling of inactive accounts after 90 days
   - Establish formal processes for requesting and approving account privileges
3. **Authentication Mechanisms**:
   - Deploy multi-factor authentication for all privileged access to the drone system
   - Implement secure password policies requiring complex passwords
   - Configure biometric authentication for physical access to ground control stations
4. **Wireless Access Controls**:

   - Implement WPA3 encryption for all wireless communications
   - Deploy wireless intrusion detection systems to monitor for unauthorized connections
   - Establish connection time restrictions for wireless access to critical functions
   - Configure automatic disconnection of inactive wireless sessions after 15 minutes

5. **Mobile Device Controls**:
   - Deploy mobile device management (MDM) solution for all devices accessing the drone system
   - Configure remote wipe capabilities for lost or stolen devices
   - Implement application whitelisting for mobile devices
   - Establish secure data synchronization procedures

1.3 Dependencies

The implementation of Access Control CCIs has dependencies on:

1. **Prior Controls**:
   - Risk assessment (RA) must be completed to inform access control policies
   - System and communications protection (SC) controls for securing information flows
   - Identification and authentication (IA) controls must be implemented before access controls
2. **System Components**:
   - Flight Control Board must support role-based access
   - Communication systems must support encrypted wireless protocols
   - Telemetry Module must enforce access controls for data transmission
   - Ground Control Station must enforce mobile device restrictions
3. **Organizational Processes**:
   - Human resources procedures must align with account management lifecycle
   - Training programs must be developed for access control awareness
   - Incident response procedures must address access control violations
   - Change management processes must incorporate access control reviews

1.4 Timeline And Milestones

The implementation timeline for Access Control CCIs is structured as follows:

1. **Phase 1 (Months 1-2)**:
   - Develop and document access control policies and procedures
   - Define roles and responsibilities for access management
   - Establish account management procedures
2. **Phase 2 (Months 3-4)**:
   - Configure account management systems
   - Implement least privilege controls
   - Deploy initial access enforcement mechanisms
   - Configure wireless access controls

3. **Phase 3 (Months 5-6)**:
    - Implement mobile device controls
    - Configure wireless monitoring systems
    - Deploy additional protections for security functions
    - Test access control mechanisms
4. **Phase 4 (Month 7)**:
    - Conduct security assessment of access controls
    - Remediate identified issues
    - Finalize documentation
    - Provide training on access control procedures

2 Audit and Accountability (AU) CCIs

2.1 Detailed Specifications

The Audit and Accountability family focuses on tracking and monitoring system activities:

- **AU-2 (Audit Events)**: Requires determining that the system can audit organization-defined events and specifying which events are to be audited.
- **AU-6 (Audit Record Review, Analysis, and Reporting)**: Requires reviewing and analyzing system audit records for indications of inappropriate or unusual activity.
- **AU-6(1) (Audit Record Review, Analysis, and Reporting — Automated Process Integration)**: Integrates audit review, analysis, and reporting processes using automated mechanisms.
- **AU-6(3) (Audit Record Review, Analysis, and Reporting — Correlate Audit Record Repositories)**: Analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

2.2 Technical Configurations and Procedural Requirements

To implement Audit and Accountability controls for the AeroTech X9 drone system:

1. **Audit Event Configuration**:
   - Configure the drone system to log all critical events including:
     - Authentication attempts (successful and failed)
     - Command executions on the drone system
     - Configuration changes to security settings
     - Access to sensitive data or functions
     - System startup and shutdown events
   - Implement secure timestamp synchronization across all system components
   - Establish audit records with sufficient detail to establish event types, timestamps, source, outcome, and identity information
2. **Audit Analysis and Reporting**:
   - Deploy automated audit analysis tools to identify suspicious patterns
   - Establish regular audit review schedules (daily for critical systems)
   - Configure automated alerting for security-relevant events
   - Implement report generation for compliance purposes
3. **Automated Process Integration**:
   - Deploy Security Information and Event Management (SIEM) system
   - Configure automated correlation rules to identify complex attack patterns
   - Implement automated incident ticket generation for suspicious events
   - Establish automated report distribution to security personnel
4. **Cross-Repository Correlation**:
   - Configure data collection from multiple sources (drone, ground control, communications)
   - Implement correlation rules across repositories
   - Deploy visualization tools for cross-system security analysis
   - Establish data normalization procedures for consistent analysis

2.3 Dependencies

Audit and Accountability controls depend on:

1. **Prior Controls**:
   - System and Communications Protection (SC) controls for secure transmission of audit data
   - Access Control (AC) controls to protect audit logs and analysis tools
   - Identification and Authentication (IA) controls to associate actions with identities
2. **System Components**:
   - SSD must have sufficient storage capacity for audit logs
   - CPU must handle audit processing without performance degradation
   - Telemetry Module must support secure transmission of audit data
   - Ground Control Station must support audit collection and analysis
3. **Organizational Processes**:
   - Incident response procedures must incorporate audit alert handling
   - Regular audit review processes must be established
   - Retention policies for audit data must be defined
   - Security personnel must be trained on audit analysis

2.4 Timeline And Milestones

Implementation timeline for Audit and Accountability controls:

1. **Phase 1 (Months 1-2)**:
   - Define auditable events for the X9 drone system
   - Establish audit storage requirements
   - Develop audit review procedures
2. **Phase 2 (Months 3-4)**:
   - Configure audit logging mechanisms
   - Deploy initial automated analysis tools
   - Implement audit storage solutions
   - Configure basic alerting rules
3. **Phase 3 (Months 5-6)**:
   - Deploy advanced SIEM capabilities
   - Implement cross-repository correlation
   - Configure advanced alerting and reporting
   - Test audit system performance
4. **Phase 4 (Month 7)**:
   - Conduct assessment of audit capabilities
   - Optimize audit performance and storage
   - Document audit procedures
   - Train personnel on audit review processes

3 Assessment Authorization and Monitoring (CA) CCIs

3.1 Detailed Specifications

The Assessment, Authorization, and Monitoring family establishes processes for assessing security controls:

- **CA-7 (Continuous Monitoring)**: Requires developing a system-level continuous monitoring strategy and implementing a continuous monitoring program.
- **CA-8 (Penetration Testing)**: Requires conducting penetration testing on organization-defined information systems or system components.

3.2 Technical Configurations and Procedural Requirements

Implementation of Assessment, Authorization, and Monitoring controls requires:

1. **Continuous Monitoring**:
   - Deploy security monitoring tools for the drone system, including:
     - Vulnerability scanners for regular system assessment
     - Configuration compliance checkers
     - Log monitoring and analysis tools
     - Security status dashboards
   - Establish monitoring metrics for security posture assessment:
     - Vulnerability remediation timeliness
     - Patch compliance levels
     - Security incident rates
     - Authentication failure rates
   - Configure automated reporting of monitoring results
   - Implement continuous monitoring of wireless communications security
2. **Penetration Testing**:
   - Establish penetration testing methodologies:
     - RF communication penetration testing
     - Physical security testing
     - Application security testing
     - Social engineering assessments
   - Develop rules of engagement for penetration testing
   - Implement secure environment for testing high-risk exploits
   - Establish remediation procedures for identified vulnerabilities

3.3 Dependencies

Implementation of Assessment, Authorization, and Monitoring controls depends on:

1. **Prior Controls**:
   - Risk Assessment (RA) controls must be implemented to inform assessment priorities
   - System and Information Integrity (SI) controls to support monitoring activities
   - Configuration Management (CM) controls for tracking system baseline

2. **System Components**:
    - Telemetry Module must support continuous monitoring
    - Flight Control Software must allow secure penetration testing
    - Communication systems must support security scanning
    - Ground Control Station must support monitoring data collection
3. **Organizational Processes**:
    - Change management procedures must incorporate security assessment
    - Vulnerability management processes must be established
    - Security assessment reporting procedures must be defined
    - Remediation tracking processes must be in place

3.4 Timeline And Milestones

Implementation timeline for Assessment, Authorization, and Monitoring controls:

1. **Phase 1 (Months 1-2)**:
    - Develop continuous monitoring strategy
    - Establish monitoring metrics and thresholds
    - Define penetration testing scope and methodology
2. **Phase 2 (Months 3-4)**:
    - Deploy initial monitoring tools
    - Establish monitoring baselines
    - Develop penetration testing rules of engagement
    - Conduct initial vulnerability assessments
3. **Phase 3 (Months 5-6)**:
    - Implement automated security reporting
    - Conduct initial penetration testing
    - Deploy security dashboards
    - Begin regular security status reporting
4. **Phase 4 (Month 7)**:
    - Finalize continuous monitoring processes
    - Document penetration testing results and remediation
    - Integrate monitoring with incident response
    - Establish ongoing assessment schedule

4 Configuration Management (CM) CCIs

4.1 Detailed Specifications

The Configuration Management family ensures secure baseline configurations and systematic control over changes to the drone system.

- CM-3 (Configuration Change Control): Requires formal change control processes.
- CM-6 (Configuration Settings): Establishes secure configuration settings for drone components.
- CM-7 (Least Functionality): Ensures only necessary functions are enabled.
- CM-8 (System Component Inventory): Maintains inventory of all system components.

4.2 Technical Configurations and Procedural Requirements

1. **Change Control System:**
   - Deploy a configuration management database (CMDB)
   - Require multi-level approvals for configuration changes
   - Integrate ticketing system for change tracking and documentation
2. **Secure Baseline Settings:**
   - Configure hardened OS images for GCS and flight modules
   - Enforce NIST and DoD STIG-compliant settings
   - Apply configuration validation during each system reboot
3. **Functionality Restriction:**
   - Disable unused ports, services, and wireless interfaces
   - Enforce strict firewall rules and endpoint lockdown
   - Monitor system activity to detect unauthorized services
4. **System Inventory:**
   - Use asset tagging for hardware, software, and firmware
   - Automate inventory reporting and change detection
   - Synchronize inventory with patch and vulnerability management tools

4.3 Dependencies

Prior Controls:

- Planning (PL) and Risk Assessment (RA)
- Identification and Authentication (IA)

System Components:

- Telemetry module and GCS
- SSD and flight firmware

Organizational Processes:

- Change Advisory Board (CAB)
- Configuration drift detection and audits

4.4 Timeline And Milestones

- **Phase 1 (Months 1–2):** Define CM policies, set up CMDB, and workflows
- **Phase 2 (Months 3–4):** Deploy configuration monitoring tools, baseline components
- **Phase 3 (Months 5–6):** Test approval and rollback processes
- **Phase 4 (Month 7):** Review/audit logs, train staff on CM lifecycle

5 Contingency Planning (CP) CCIs

5.1 Detailed Specifications

Contingency Planning ensures the AeroTech X9 can recover from disruptions or failures. Applicable controls include:

- **CP-2:** Contingency Plan
- **CP-8:** Telecommunications Services
- **CP-10:** System Recovery and Reconstitution
- **CP-10(1):** Contingency Plan Testing
- **CP-13:** Alternative Security Mechanisms

5.2 Technical Configurations and Procedural Requirements

1. **Contingency Plan Development:**
   - Define mission-essential components and RTO/RPO
   - Map dependencies and suppliers
2. **Telecommunication Redundancy:**
   - Implement SATCOM failover and VPN-based fallback
3. **Recovery and Testing:**
   - System snapshots for reconstitution
   - Biannual failover and tabletop testing
4. **Alternative Mechanisms:**
   - Manual override for emergency landing
   - Encrypted USB-based field recovery

5.3 Dependencies

Prior Controls:

- Risk Assessment (RA)
- Configuration Management (CM)

System Components:

- Ground Control Station and telemetry modules

Organizational Processes:

- IR team integration
- Training and compliance with DoD standards

5.4 Timeline And Milestones

- **Phase 1 (Months 1–2):** Draft contingency plan, identify backups
- **Phase 2 (Months 3–4):** Deploy redundancy systems
- **Phase 3 (Months 5–6):** Conduct recovery drills
- **Phase 4 (Month 7):** Finalize procedures, train response teams

6 Identification and Authentication (IA) CCIs

6.1 Detailed Specifications

The Identification and Authentication family ensures only authorized users access drone systems:

- **IA-2:** Unique IDs and multifactor authentication
- **IA-2(8):** PKI smartcards for privileged access
- **IA-3:** Device authentication and management
- **IA-4:** Replay attack protection
- **IA-5:** Strong password/credential policy

6.2 Technical Configurations and Procedural Requirements

1. **User Authentication:**
   - Use CAC/PIV smartcards and 2FA for remote access
2. **Device Authentication:**
   - Mutual authentication using certificates
   - Unique crypto IDs per component
3. **Credential Management:**
   - Rotate passwords every 60 days
   - Use FIPS 140-2 compliant vault
   - Monitor for lockout/brute-force attempts
4. **Replay Attack Protection:**
   - Implement session tokens and nonce challenges
   - Enforce telemetry encryption with sequencing

6.3 Dependencies

Prior Controls:

- Access Control (AC)
- Risk Assessment (RA)

System Components:

- TPMs, GCS, and UAV radios for PKI support

Organizational Processes:

- Align provisioning with HR policies
- Schedule periodic access reviews

6.4 Timeline And Milestones

- **Phase 1 (Months 1–2):** Define ID policies, map roles
- **Phase 2 (Months 3–4):** Deploy 2FA and PKI
- **Phase 3 (Months 5–6):** Implement replay protection
- **Phase 4 (Month 7):** Conduct audits and finalize training

7 Incident Response (IR) CCIs

7.1 Detailed Specifications

The Incident Response family ensures timely detection, reporting, and handling of incidents for the X9 UAV and GCS:

- **IR-4(5) Incident Handling — Automatic Disabling of System**: Implement a configurable capability to automatically disable the system if organization-defined security violations are detected.

7.2 Technical Configurations and Procedural Requirements

To implement Incident Response controls for the X9 system:

1. **Incident Handling and Notification Configuration**:
    - *CCI-000831*: Capability to automatically disable the system.
        - Configure X9 UAV and GCS to detect security violations (e.g., unauthorized access attempts, tampered firmware).
        - Implement automatic shutdown triggers (e.g., after 3 failed authentication attempts or detection of malicious code).
        - Log shutdown events with timestamps, violation type, and system state.
        - Test disable functionality in a controlled environment.

7.3 Dependencies

Incident Response controls depend on:

1. **Prior Controls**:
    - IR-4 (Incident Handling) for response processes.
    - IR-6 (Incident Reporting) for external reporting.
    - IR-8 (Incident Response Planning) for planning framework.
    - SC-13 (Cryptographic Protection) for secure notification channels.
2. **System Components**:
    - GCS must support encrypted communication and shutdown commands.
    - SSD must store notification and shutdown logs securely.
    - CPU must process real-time incident alerts and disable actions without latency.
    - RF/SATCOM must transmit notifications reliably.
3. **Organizational Processes**:
    - Supply chain relationships must be established.
    - Incident response team must be trained on notification and shutdown protocols.
    - Legal agreements (MOUs) must be in place with suppliers.

7.4 Timeline And Milestones

Implementation timeline for IR controls:

1. **Phase 1 (Months 1-2)**:
   - Define security violations and notification requirements.
   - Draft MOUs with supply chain entities.
2. **Phase 2 (Months 3-4)**:
   - Configure secure communication channels and shutdown triggers.
   - Sign agreements and deploy notification templates.
3. **Phase 3 (Months 5-6)**:
   - Train X9 incident response team.
4. **Phase 4 (Month 7)**:
   - Assess notification and shutdown effectiveness.
   - Document procedures in X9 IR Plan.

8 Media Protection (MP) CCIs

8.1 Detailed Specifications

The Media Protection family ensures secure disposal of X9 data and components.
Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here.

9 Physical and Environmental Protection (PE) CCIs

9.1 Detailed Specifications

The Physical and Environmental Protection family safeguards X9 hardware. Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here.

10 Planning (PL) CCIs

10.1 Detailed Specifications

The Planning family includes the following key controls that must be implemented for the AeroTech X9 drone system:

- PL-1 (Policy and Procedures): Requires developing, documenting, and disseminating planning policies that address purpose, scope, roles, and responsibilities.
- PL-2 (System Security Plan): Requires creating a system security plan that describes system boundaries, security controls, and implementation details.
- PL-2(1) (System Security Plan — Coordination): Requires coordinating security planning activities with organizational stakeholders.
- PL-2(2) (System Security Plan — Approval Process): Requires formal approval processes for the system security plan by designated officials.
- PL-2(3) (System Security Plan — Updates): Mandates periodic updates to the security plan to reflect changes in the system or environment.
- PL-3 (Rules of Behavior): Establishes rules of behavior for users accessing the drone system, including acceptable use policies.
- PL-4 (Information Security Architecture): Defines the security architecture for the drone system, including data flows and integration points.
- PL-4(1) (Information Security Architecture — Integration): Requires integrating security architecture into system design processes.
- PL-5 (System Inventory): Ensures accurate inventory of all system components, including hardware, software, and firmware.
- PL-6 (Central Management): Establishes centralized management processes for planning activities across organizational units.

10.2 Technical Configurations and Procedural Requirements

To implement these controls for the AeroTech X9 drone system, the following technical configurations and procedures must be established:

- Security Planning Policies:

  Develop comprehensive security planning policies at organizational and system levels.

  Implement annual review procedures to ensure policies remain relevant.

  Establish formal approval workflows for policy updates.

- System Security Plan:

  Document system boundaries, interfaces, and data flows in detail.

  Configure automated tools to track updates to the security plan.

  Implement version control mechanisms to maintain historical records of changes.

- Rules of Behavior:

  Define acceptable use policies for all users accessing the drone system.

  Develop training programs to ensure compliance with rules of behavior.

- Information Security Architecture:

  Use modeling tools to design and validate security architecture against organizational standards.

  Implement secure data flow diagrams to identify vulnerabilities in communication pathways.

10.3 Dependencies

The implementation of Planning CCIs has dependencies on:

- Prior Controls:

  Risk Assessment (RA) controls must inform planning activities by identifying threats and vulnerabilities.

  Configuration Management (CM) controls must provide baseline information for planning purposes.

- System Components:

  Flight Control Software must align with documented security plans and architectures.

  Communication systems must support secure data flows as defined in the security architecture.

- Organizational Processes:

  Governance frameworks must support centralized planning activities across departments.

  Stakeholder coordination processes must ensure alignment with mission objectives and compliance requirements.

10.4 Timeline And Milestones

The implementation timeline for Planning CCIs is structured as follows:

- Phase 1 (Months 1–2)

  Develop and document planning policies and procedures.

  Define roles and responsibilities for planning activities.

  Draft initial system security plan documentation.

- Phase 2 (Months 3–4)

  Validate rules of behavior with stakeholders.

  Design initial information security architecture.

  Conduct inventory of system components.

- Phase 3 (Months 5–6)

  Update system security plan based on testing results.

  Integrate planning outputs into operational workflows.

  Finalize centralized management processes.

- Phase 4 (Month 7)

  Conduct assessment of planning deliverables.

  Remediate identified gaps or inconsistencies.

  Provide training on planning policies and procedures.

11 Program Management (PM) CCIs

11.1 Detailed Specifications

The Program Management family includes the following key controls for the AeroTech X9 drone system:

- PM-1 (Information Security Program Plan): Requires developing an organization-wide security program plan outlining roles, compliance, and coordination.
- PM-2 (Information Security Program Leadership Role): Designates leadership roles for security program oversight and accountability.
- PM-3 (Information Security Resources): Allocates budgetary, personnel, and technical resources for security implementation.
- PM-4 (Plan of Action and Milestones): Documents remediation timelines for security weaknesses.
- PM-5 (System Inventory): Maintains an inventory of organizational systems, including hardware, software, and ownership.
- PM-5(1) (System Inventory — Automated Tracking): Implements automated tools for real-time inventory updates.
- PM-6 (Security Measures Metrics): Defines quantitative metrics to evaluate security control effectiveness.
- PM-7 (Enterprise Architecture): Aligns security architecture with organizational mission and data flows.
- PM-7(1) (Enterprise Architecture — Integration): Integrates security architecture into system development lifecycle.
- PM-8 (Critical Infrastructure Plan): Identifies and protects systems critical to organizational missions.
- PM-9 (Risk Management Strategy): Establishes a risk management framework tailored to organizational objectives.
- PM-10 (Security Authorization Process): Manages system authorization through continuous monitoring.
- PM-11 (Mission/Business Process Definition): Defines mission-critical processes and associated security needs.
- PM-12 (Insider Threat Program): Implements cross-disciplinary teams to detect and mitigate insider threats.
- PM-13 (Security Workforce): Ensures personnel have qualifications to manage security risks.
- PM-14 (Testing, Training, and Monitoring): Conducts security testing, training, and monitoring activities.
- PM-15 (Contacts with Groups/Associations): Coordinates with external entities for threat intelligence sharing.
- PM-16 (Threat Awareness Program): Implements organization-wide threat awareness initiatives.
- PM-16(1) (Threat Awareness — Social Engineering): Focuses on mitigating social engineering risks.
- PM-17 (Supply Chain Risk Management): Addresses risks in third-party vendors and suppliers.
- PM-18 (Privacy Program): Ensures compliance with privacy regulations and data protection.

- PM-19 (Compliance Program): Monitors adherence to legal, regulatory, and contractual obligations.
- PM-20 (Disposal/Transition Processes): Defines secure disposal or transition of systems/data.
- PM-20(1) (Disposal/Transition — Data Retention): Establishes data retention policies for archived information.
- PM-21 (Security Automation): Deploys tools for automated security monitoring and compliance.
- PM-22 (Security Policy Updates): Requires annual review and updates to security policies.
- PM-23 (Data Governance): Implements controls for data classification, handling, and storage.
- PM-24 (Incident Response Coordination): Integrates incident response with organizational processes.
- PM-25 (Vulnerability Management): Tracks and remediates vulnerabilities across systems.
- PM-26 (Third-Party Oversight): Monitors third-party compliance with security requirements.
- PM-27 (Contingency Planning): Develops plans for continuity of operations during disruptions.
- PM-28 (Physical Security): Protects facilities housing critical systems and data.
- PM-29 (System Interconnections): Manages security for interconnected systems and data sharing.
- PM-30 (Audit Logging): Configures audit logs for monitoring user activities and system events.
- PM-31 (Configuration Management): Enforces secure configurations and change control processes.
- PM-32 (Cybersecurity Framework Integration): Aligns security controls with NIST CSF categories.

11.2 Technical Configurations and Procedural Requirements

To implement PM controls for the AeroTech X9 drone system:

- Program Governance:

  Deploy centralized dashboards for security program oversight.

  Configure automated tools for inventory tracking (PM-5(1)) and compliance reporting.

- Risk Management:

  Integrate threat intelligence feeds into risk assessments (PM-16).

  Conduct tabletop exercises for insider threat scenarios (PM-12).

- Workforce Security:

  Implement role-based training programs for security personnel (PM-13).

  Deploy SIEM tools for automated monitoring and alerting (PM-21).

- Third-Party Management:

  Establish vendor risk assessment workflows (PM-17, PM-26).

  Enforce contractual security requirements for suppliers.

11.3 Dependencies

Implementation of PM CCIs depends on:

- Prior Controls:

  Planning (PL): Security plans (PL-2) inform program governance (PM-1).

  Risk Assessment (RA): Risk registers guide PM-9 strategy development.

- System Components:

  Drone Telemetry Module: Must support audit logging (PM-30) and secure interconnections (PM-29).

  Ground Control Station: Requires role-based access aligned with PM-13 workforce roles.

- Organizational Processes:

  Change management must integrate with PM-31 (configuration management).

  Incident response plans must align with PM-24 coordination requirements.

11.4 Timeline And Milestones

The implementation timeline for PM CCIs is structured as follows:

- Phase 1 (Months 1–2):

  Develop security program plan (PM-1) and inventory systems (PM-5).

  Define mission-critical processes (PM-11) and risk strategy (PM-9).

- Phase 2 (Months 3–4):

  Deploy automated inventory tools (PM-5(1)) and governance dashboards.

  Conduct workforce training (PM-13) and initiate third-party assessments (PM-17).

- Phase 3 (Months 5–6):

  Implement SIEM for automated monitoring (PM-21).

  Test insider threat response (PM-12) and update policies (PM-22).

- Phase 4 (Month 7):

  Finalize documentation and integrate PM controls with NIST CSF (PM-32).

  Conduct security assessment and remediate gaps.

12 Risk Assessment (RA) CCIs

12.1 Detailed Specifications

The Risk Assessment family includes the following key controls for the AeroTech X9 drone system:

- RA-1 (Policy and Procedures): Requires developing risk assessment policies addressing scope, roles, and compliance requirements.
- RA-2 (Security Categorization): Categorizes systems/data based on impact levels (low, moderate, high).
- RA-2(1) (Security Categorization — Impact Analysis): Conducts mission/business impact analyses to inform categorization.
- RA-3 (Risk Assessment): Identifies threats, vulnerabilities, and risks to organizational operations.
- RA-3(1) (Risk Assessment — Threat Intelligence): Integrates threat intelligence from external sources.
- RA-3(2) (Risk Assessment — Vulnerability Monitoring): Tracks vulnerabilities in hardware, software, and configurations.
- RA-3(3) (Risk Assessment — Supply Chain Risks): Assesses risks from third-party vendors and suppliers.
- RA-3(4) (Risk Assessment — Predictive Analytics): Uses AI/ML tools to predict emerging risks.
- RA-4 (Risk Assessment Update): Mandates periodic reassessment of risks based on system/environmental changes.
- RA-5 (Vulnerability Monitoring): Scans systems for vulnerabilities and prioritizes remediation.
- RA-5(1) (Vulnerability Monitoring — Automation): Deploys automated tools for continuous vulnerability detection.
- RA-5(2) (Vulnerability Monitoring — Update Frequency): Requires daily scans for critical systems.
- RA-5(3) (Vulnerability Monitoring — Breadth/Depth): Expands scans to include firmware and APIs.
- RA-5(4) (Vulnerability Monitoring — Privileged Access): Restricts vulnerability scanning to authorized users.
- RA-5(5) (Vulnerability Monitoring — Historical Data): Maintains historical records of vulnerabilities.
- RA-5(6) (Vulnerability Monitoring — Trend Analysis): Analyzes vulnerability trends to predict risks.
- RA-5(7) (Vulnerability Monitoring — False Positives): Implements processes to reduce false positives.
- RA-5(8) (Vulnerability Monitoring — Penetration Testing): Correlates scan results with penetration testing.
- RA-5(9) (Vulnerability Monitoring — Public Disclosure): Monitors public sources for new vulnerabilities.
- RA-5(10) (Vulnerability Monitoring — Incident Response): Integrates findings into incident response workflows.
- RA-5(11) (Vulnerability Monitoring — Risk Scoring): Assigns risk scores based on exploit likelihood/impact.
- RA-6 (Technical Surveillance Countermeasures): Detects and mitigates unauthorized surveillance.

- RA-7 (Risk Response): Defines mitigation, transfer, acceptance, or avoidance strategies for identified risks.
- RA-8 (Privacy Impact Assessment): Evaluates risks to personally identifiable information (PII).
- RA-9 (Criticality Analysis): Prioritizes risks to mission-critical components (e.g., flight control systems).
- RA-10 (Threat Hunting): Proactively searches for advanced threats within the drone ecosystem.

12.2 Technical Configurations and Procedural Requirements

To implement RA controls for the AeroTech X9 drone system:

- Risk Assessment Tools:

  Deploy vulnerability scanners (e.g., Tenable, Qualys) with configurations for firmware/API coverage (RA-5(3)).

  Integrate threat intelligence platforms (RA-3(1)) with SIEM for real-time alerts.
- Vulnerability Management:

  Configure automated daily scans for critical systems (RA-5(2)) and role-based access for scanners (RA-5(4)).

  Implement risk scoring models (RA-5(11)) to prioritize remediation based on exploitability and impact.
- Threat Hunting:

  Deploy endpoint detection and response (EDR) tools to identify advanced threats (RA-10).

  Conduct red team exercises simulating drone-specific attack vectors (e.g., GPS spoofing).
- Supply Chain Risks:

  Assess third-party vendors for compliance with security requirements (RA-3(3)).

  Require vendors to disclose vulnerabilities in components (e.g., telemetry modules).

12.3 Dependencies

Implementation of RA CCIs depends on:

- Prior Controls:

  Planning (PL): Security plans (PL-2) define risk assessment scope.

  Audit and Accountability (AU): Audit logs (AU-2) inform vulnerability trends (RA-5(6)).
- System Components:

  Flight Control Software: Must support vulnerability scanning without disrupting operations (RA-5).

  Communication Systems: Require encryption to mitigate risks identified in RA-7.
- Organizational Processes:

  Incident response procedures must incorporate threat hunting findings (RA-10).

  Vendor contracts must include vulnerability disclosure clauses (RA-3(3)).

12.4 Timeline And Milestones

The implementation timeline for RA CCIs is structured as follows:

- Phase 1 (Months 1–2):

  Develop risk assessment policies (RA-1) and categorize systems (RA-2).

  Conduct mission impact analysis (RA-2(1)) and baseline vulnerability scans (RA-5).

- Phase 2 (Months 3–4):

  Deploy automated vulnerability tools (RA-5(1)) and integrate threat intelligence (RA-3(1)).

  Assess supply chain risks (RA-3(3)) and define risk response strategies (RA-7).

- Phase 3 (Months 5–6):

  Conduct predictive risk analysis (RA-3(4)) and penetration testing (RA-5(8)).

  Initiate threat hunting activities (RA-10) and update risk assessments (RA-4).

- Phase 4 (Month 7):

  Finalize risk documentation and integrate findings into incident response (RA-5(10)).

  Train staff on risk management workflows and tools.

13 System and Services Acquisition (SA) CCIs

13.1 Detailed Specifications

- SA-10 (Developer Configuration Management): Requires the developer of the system, component, or service to perform proper configuration management, and to document any organization-approved changes to the configuration.

- SA-11 (Developer Testing and Evaluation): Requires the developer of the system, component, or service to implement a test plan and evaluate security/privacy control assessments at all post-design stages of the system's life cycle.

- SA-11(1) (Developer Testing and Evaluation — Static Code Analysis): Requires the developer of the system, component, or service to employee Static Code Analysis Tools to identify and document common flaws.

13.2 Technical Configurations and Procedural Requirements

- For SA-10, all developers must use a version-controlled repository (e.g., Git with signed commits) with enforced change approval workflows. Configuration baselines must be documented in configuration control documents and reviewed quarterly.

- For SA-11, test cases must cover all functional and non-functional requirements, including security and privacy. Developers must run automated unit and integration tests with coverage reports.

- For SA-11(1), CI pipelines must include static code analysis via tools like CodeQL or SonarQube, and all critical issues must be resolved before merging to protected branches. Output must be retained for 1 year.

13.3 Dependencies

- SA-10 depends on CM-2 (Baseline Configuration) and CM-3 (Configuration Change Control).

- SA-11 requires alignment with CA-2 (Control Assessments) and SA-15 (Development Process, Standards, and Tools).

- SA-11(1) is enhanced by SI-7 and SI-10 for integrity checks and mitigations of flaws identified during static analysis.

13.4 Timeline And Milestones

- **Phase 1 (1–2 months)**: Finalize development configuration management policies and select approved tools for version control, change management, and static analysis.

- **Phase 2 (3–4 months)**: Integrate configuration control workflows and automated testing into CI/CD pipelines.

- **Phase 3 (5–6 months)**: Conduct internal audit on compliance with SA-10 and SA-11; refine test plans and developer workflows based on findings.

- **Phase 4 (7+ months)**: Institutionalize review cycles and reporting for change logs and testing results across all development teams.

14 System and Communications Protection (SC) CCIs

14.1 Detailed Specifications

- SC-5 (Denial-of-service Protection): Implement controls to to protect against and limit the effects of a denial-of-service event.
- SC-7 (Boundary Protection): Monitor and control communications from external interfaces to the system. Use only managed sub-networks for the publicly accessible system components and only allow access through managed interfaces to provide protection of boundaries.
- SC-8 (Transmission Confidentiality and Integrity): Employ controls to protect the confidentiality and integrity of information being transmitted through devices to prevent critical info being leaked.
- SC-12 (Cryptographic Key Establishment and Management): Establish and manage cryptographic keys in accordance to organization-defined requirements relating to key generation, distribution, storage, access, and destruction.
- SC-16 (Transmission of Security and Privacy Attributes): Associate organization-defined security/privacy attributes to information that is exchanged between systems and components.
- SC-25 (Thin Nodes): Employ minimal functionality and information storage on components. Least-privilege.
- SC-28 (Protection of Information at Rest): Protect the confidentiality and integrity of critical information in rest on components like hard drives.
- SC-38 (Operations Security): Employ operations security controls to protect key organizational information during system's development life cycle.
- SC-39 (Process Isolation): Maintain a separate domain for executing each system execution process.
- SC-40 (Wireless Link Protection): Protect external and internal wireless links from signal parameter attacks that could be used to gain information.

14.2 Technical Configurations and Procedural Requirements

- SC-5: Implement rate-limiting and blackhole routing for suspicious traffic using firewalls and WAFs.
- SC-7: Use firewalls with stateful inspection and conduct monthly access control reviews. Network segmentation enforces managed interfaces.
- SC-8 and SC-12: Employ TLS 1.3 for all data in transit and FIPS 140-3 validated key management modules (e.g., AWS KMS).
- SC-16: Use secure API gateways that tag metadata attributes to messages.
- SC-25: IoT components will be delivered with hardened firmware and locked configurations with minimal services enabled.
- SC-28: Data at rest must be encrypted using AES-256 with centralized key rotation policies.
- SC-38: Perform OPSEC risk assessments quarterly during development sprints.
- SC-39: Containerized applications run in isolated namespaces with SELinux or AppArmor enforcing isolation.
- SC-40: Wireless access must use WPA3 Enterprise with signal jamming and rogue AP detection tools.

14.3 Dependencies

- SC-5 is supported by IR-4 (Incident Handling) and SC-6 (Resource Priority).
- SC-7, SC-8, and SC-12 relate to AC-4 (Information Flow Enforcement) and MP-5 (Media Transport Protection).
- SC-25 and SC-28 are dependent on system hardening (SI-7) and encryption control standards (SC-12).
- SC-39 and SC-40 align with PE-18 (Location of System Components) and PL-8 (Security and Privacy Architectures).

14.4 Timeline And Milestones

- **Phase 1 (1–2 months)**: Deploy DoS protection mechanisms, configure firewall rule sets, and initiate wireless access reviews.
- **Phase 2 (3–4 months)**: Implement TLS 1.3 for data-in-transit and encrypt all data-at-rest using AES-256; isolate containers and VMs.
- **Phase 3 (5–6 months)**: Apply minimal-function configurations to thin nodes and establish process isolation using OS-level controls.
- **Phase 4 (7+ months)**: Finalize operations security documentation and conduct end-to-end penetration testing of boundary protections.

15 System and Information Integrity (SI) CCIs

15.1 Detailed Specifications

- SI-2 (Flaw Remediation): Incorporates identifying, reporting, and correcting system flaws.
- SI-4 (System Monitoring): Incorporates system monitoring to detect potential/active attacks, unauthorized connections or system use, organizational essential information, anomalies, and sensitivity is not high enough to get flag false-positives.
- SI-7 (Software, Firmware, and Information Integrity): Employs integrity verification tools to detect unauthorized changes to software, firmware, or information and take action if detected.
- SI-7(1) (Software, Firmware, and Information Integrity — Integrity Checks): Performs integrity checks using integrity verification tools to detect anomalies.

15.2 Technical Configurations and Procedural Requirements

- SI-2: Implement automated patching systems (e.g., WSUS, yum/dnf, pip audit) with SLA-based remediation tracking.
- SI-4: Deploy continuous monitoring tools (e.g., Splunk, ELK, Wazuh) with real-time alerting and anomaly detection.
- SI-7 and SI-7(1): Use file integrity monitoring (FIM) tools (e.g., Tripwire, AIDE) to baseline and verify critical binaries and libraries on a weekly basis.

15.3 Dependencies

- SI-2 relies on CM-4 (Security Impact Analysis) and SA-22 (Unsupported System Components).
- SI-4 integrates with AU-6 (Audit Review, Analysis, and Reporting) and IR-5 (Incident Monitoring).
- SI-7 depends on SC-28 (Protection of Information at Rest) and SC-12 (Cryptographic Key Management).

15.4 Timeline And Milestones

- **Phase 1 (1–2 months)**: Deploy patch management systems and vulnerability scanning across infrastructure and development environments.
- **Phase 2 (3–4 months)**: Integrate logging, anomaly detection, and threat intelligence feeds with security monitoring platforms.
- **Phase 3 (5–6 months)**: Configure integrity checking tools and develop baseline files for monitoring key binaries and libraries.
- **Phase 4 (7+ months)**: Review monitoring effectiveness, tune false positives, and establish long-term audit and integrity verification cadence.