

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

<System Name> (<System Acronym>)

Facilities Compliance  
Checklist

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Nate Lee Andrew Bennett Ernie Riviere | Initial release of MITRE ACT templates and work aids. |

Purpose

This questionnaire provides a suggested *guide* for the assessor to use when interviewing system personnel as part of an ACT Security Assessment. It contains a large set of interview questions that the assessor *might* ask. Not all questions are required to be asked and/or answered, and each question might be presented to multiple system personnel in different roles. The assessor is free to deviate from this questionnaire in whatever manner they deem appropriate based on the specific context of the assessment and the interview.

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Facility Visit Details

Table . Facility Visit Logistics

|  |  |
| --- | --- |
| Date of Facility Visit |  |
| Location of Facility |  |

Table . Assessor(s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| Facilities Assessor |  | Assessment Team |  |  |

Table . Facility Visit Participants

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Organization | Phone Number | Email Address |
| Assessment POC |  |  |  |  |
| Application Developer |  |  |  |  |
| Business Owner |  |  |  |  |
| Cloud Services Administrator |  |  |  |  |
| Configuration Manager |  |  |  |  |
| Contingency Planning Manager |  |  |  |  |
| Contracting Officer (COR) |  |  |  |  |
| Cyber Risk Advisor (CRA) |  |  |  |  |
| Database Administrator |  |  |  |  |
| Datacenter/Facilities Manager |  |  |  |  |
| Development Lead |  |  |  |  |
| Firewall Administrator |  |  |  |  |
| Human Resources Manager |  |  |  |  |
| Incident Handling Manager |  |  |  |  |
| Information System Security Officer (ISSO) / Manager (ISSM) |  |  |  |  |
| ISSO/ISSM - Contractor |  |  |  |  |
| Mainframe Administrator |  |  |  |  |
| Media Custodian |  |  |  |  |
| Middleware Utilities Administrator |  |  |  |  |
| Network Administrator |  |  |  |  |
| Privacy Subject Matter Expert (PSME) |  |  |  |  |
| Program Manager |  |  |  |  |
| Security Utilities Administrator |  |  |  |  |
| System Administrator |  |  |  |  |
| System Owner |  |  |  |  |
| Training Manager |  |  |  |  |
| Virtualization Administrator |  |  |  |  |

Topics Quick Reference

[1. Physical and Environmental Protection (PE) 1](#_Toc199482364)

[2. Maintenance (MA) 5](#_Toc199482365)

[3. Media Protection (MP) 6](#_Toc199482366)

# 

# Physical and Environmental Protection

Physical and Environmental Protection seeks to safeguard information systems, equipment, and facilities from physical threats and environmental hazards to ensure system availability, confidentiality, and integrity.

|  |  |  |
| --- | --- | --- |
| Control(s) | Check(s) | Notes & Comments |
| PE-1 | * What is the documented, physical, and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance? * Review the policy. |  |
| PE-2 | * How is physical access into the data center limited to those individuals whose primary business functions require them to have access? Observe. * What lists of people exist that are allowed in the building and that are allowed in the server room and/or wiring closets? * How do you log who enters the facility and who enters the server room? Are they separate lists? * How often are authorized access lists reviewed? (365 for Low, 180 for Moderate, 90 days for High impact systems) and by whom? * How are the entry logs maintained after review? How and by whom? * How are authorized personnel, contractors, and visitors physically identified? Do they wear visible identification? |  |
| PE-3 | * How are the doors and windows protected? Observe any locks on all exterior doors and windows. * How does the facility respond if one of the doors or windows were to be compromised? Automatic Notification? * How are servers physically secured? Are they stored in a physically secure environment (i.e., locked racks in a server room or in locked server closet)? Observe and note. * For PII only, what are the two physical barriers required to access PII under normal security? Are they one of the following: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container? Observe and note. * How is CMS protected information containerized/segregated in areas where other than authorized employees may have access after hours? * If badges are used, describe their use. Are there different levels or types of badges that allow access to different parts of the facility? * How are the badge swipes tracked as part of PE-2? * What reports exist for tracking access? Request copies. * How often are keys changed and who maintains the keys? |  |
| PE-4 | * How is access to telephone lines and switches behind locked doors, wiring closets limited? Observe and note. |  |
| PE-5 | * Observe if it is possible to see desktop monitors from outside the facility. |  |
| PE-6 | * How does the organization monitor physical access to the facility? Observe and note. * How does the facility use cameras? Observe and note. * How does the facility use motion sensors or pressure plates? Observe and note. * How are 24-hour security guards, etc. used? Observe and note. |  |
| PE-8 | * What is the process for visitors entering the facility? Do they sign in? What is required? Request a copy or observe. * What is required of visitors entering the server room/data center? How are they monitored? Do they sign in? Observe and note. * Observe sign-in sheet(s). Do they include (i) person visiting name and organization; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) person visited name and organization? |  |
| PE-9 | * What public access to infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets exists? Observe and note. * When in the server room, how is the cabling on the floor maintained? Observe if it is neat or unkempt. * How is third-party entity maintenance in the server room handled? |  |
| PE-10 | * Observe immediately upon entering the server room, standing at the door, look around for the emergency power switch. Is it in view? * Is there a sign obviously pointing out the location of the shut-off? Observe and note. * Is the emergency shut-off switch location visible from all entrances? |  |
| PE-11 | * Identify the UPS or emergency power generators. Observe and note. * What load can the UPS/generators handle? For how long? * How often is the UPS equipment tested? Who tests it? |  |
| PE-12 | * What emergency lighting exists in the hallways? Observe and note. * What emergency lights are in the offices? * What emergency lights are in the server room/data center? Observe and note. |  |
| PE-13 | * Where are the fire extinguishers located? Have personnel ever used this type of fire extinguisher? Observe and note. * If there are fire extinguishers, when was the last time they were tested? Are they still in good working condition? * What automatic fire suppression system (i.e., sprinklers) is present in server room? Observe and note. * Do the sprinklers use water or Halon? * Are they dry pipe or wet pipe? * How many zones? * When was the last time the sprinklers were tested? Who tested them? * What are the notification procedures for emergency responders? Are they notified automatically in the event of a fire? |  |
| PE-14 | * In the server room/data center, how are temperature and humidity monitored? Observe and note. * How are administrators notified if the temperature or humidity goes outside acceptable bounds—are emails, texts or pages send? |  |
| PE-15 | * In the server room/data center, is there a raised floor? Observe and note. * How is monitoring done to determine if there is water on the floor in the server room/data center? Observe and note. * Are there any overhead pipes that may leak and cause water damage? Observe and note. * Describe any training personnel receive related to shutting off the water supply? |  |
| PE-16 | * How are deliveries done to the server room/data center? * How are records of the delivery or service call logged and traced? Review the records. |  |
| PE-17 | * What is the alternate work site for the server room/data center, personnel, and/or managerial personal? * What happens if/when the facility is suddenly unusable? |  |
| PE-18 | * Are components positioned within the facility to minimize potential damage from physical/environmental hazards? |  |

# Maintenance

Maintenance ensures that information systems are properly maintained to support security and operational effectiveness throughout their lifecycle.

|  |  |  |
| --- | --- | --- |
| Control(s) | Check(s) | Notes & Comments |
| MA-2 | * How are maintenance activities controlled, to include routine, scheduled maintenance, and repairs? * How is maintenance done, onsite or remotely? * How is equipment serviced, on site or removed to another location? * Describe the management authorization for removal that is required before any information processing equipment can be removed and used outside of your premises. * What type of records are maintained (i) date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable? Observe and note. |  |
| MA-3 | * What agreements or arrangements regarding diagnostic equipment and software that vendors may bring onsite exist? Observe and note. * How is access to tools restricted to maintenance personnel? |  |
| MA-4 | * What ability do vendors have to perform remote diagnostics and maintenance? * How is remote diagnostics and maintenance authorized, monitored, and controlled? Review procedures. * Are records for remote maintenance maintained? Examine the records. |  |
| MA-5 | * Is there a list of personnel authorized to perform maintenance on the information systems? Examine the list. * Who maintains it and who has access to it? * How are maintenance personnel verified? |  |
| MA-6 | * What spare parts are stored onsite? Where? Observe the area. * Describe the service level agreements with maintenance vendors (turn-around time). Review agreements. * What is the documented maintenance schedule? Examine the schedule. |  |

# Media Protection

Media Protection safeguards system media—both digital and physical—to prevent unauthorized access, use, disclosure, modification, or destruction of sensitive information.

|  |  |  |
| --- | --- | --- |
| Control(s) | Check(s) | Notes & Comments |
| MP-2 | * How is access to media storage areas restricted to authorized personnel including offsite storage? Observe and note. * How is access audited? |  |
| MP-3 | * Describe media labeling. Are external labels affixed to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings of the information? Observe and note. |  |
| MP=4 | * How is sensitive information (e.g., PII, PHI, and FTI) contained in electronic media (e.g., backup or thumb drive) that you control/access? * How is the information system media protected? By cryptography (NIST SP 800-66 has guidance)? |  |
| MP-5 | * How is information system media (backups, thumb drives, etc.) protected during transport outside of controlled areas (e.g., locked container, turtle shell, encryption)? Observe and note. * What restrictions are in place for transport of such media to authorized personnel? * For backups, how is the transport of media logged and documented? |  |
| MP-6 | * How is information system media, both digital and non-digital, sanitized prior to disposal or release for reuse? * Is electronic media sanitized in accordance with best practices (NSA Guidance (Media Destruction Guidance) and NIST SP 800-88 (Guidelines for Media Sanitization))? * How is sanitization tracked and documented? Request a copy of the log. |  |
| MP-7 | * How is information system media restricted to prohibit access to ports, insertion (USB, drives, removal, etc.) for read/write access of data? * If applicable, how is the identify of a removable device owner obtained, and audited, captured in audit logs? |  |