| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-17** | REMOTE ACCESS | |
| **AC-17.1**  **AC-17.1.1**  **AC-17.1.2**  **AC-17.1.3**  **AC-17.1.4**  **AC-17.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization documents allowed methods of remote access to the information system;* 2. *the organization establishes usage restrictions and implementation guidance for each allowed remote access method;* 3. *the organization monitors for unauthorized remote access to the information system;* 4. *the organization authorizes remote access to the information system prior to connection; and* 5. *the organization enforces requirements for remote connections to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with remote access authorization, monitoring, and control responsibilities].  **Test**: [*select from:* Remote access methods for the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2  concurrent controls: AC-3, AC-4, AC-18, AC-20, AU-2, AU-3, AU-6, AU-7, AU-12, AU-14,  CM-8, IA-2, IA-3, IA-8, MA-4, SC-7, SI-4  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **AC-17.1.1.1** | | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the allowed methods of remote access to the information system. |
|  | |  |
| **AC-17.1.2.1** | | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the usage restrictions and implementation guidance for each allowed remote access method identified in AC-17.1.1.1. |
|  | |  |
| **AC-17.1.3.1** | | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to monitor for unauthorized remote access to the information system. |
| **AC-17.1.3.2** | | **Examine** remote access monitoring records for an agreed-upon [*basic*] sample of allowed remote access methods; [*reviewing*] for evidence that the measures identified in AC-17.1.3.1 are being applied to monitor unauthorized remote access to the information system. |
| **AC-17.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with remote access monitoring responsibilities; [*reviewing*] for further evidence that the measures identified in AC-17.1.3.1 are being applied. |
|  | |  |
| **AC-17.1.4.1** | | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to authorize remote access to the information system prior to connection. |
| **AC-17.1.4.2** | | **Examine** authorization approvals for an agreed-upon [*basic*] sample of remote access connections to the information system; [*reviewing*] for evidence that the measures identified in AC-17.1.4.1 are being applied to authorize remote access prior to connection. |
| **AC-17.1.4.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with remote access authorization responsibilities; [*reviewing*] for further evidence that the measures identified in AC-17.1.4.1 are being applied. |
|  | |  |
| **AC-17.1.5.1** | | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to enforce requirements for remote connections to the information system. |
| **AC-17.1.5.2** | | **Examine** configuration settings and associated documentation for an agreed-upon [*basic*] sample of remote access connections to the information system; [*reviewing*] for evidence that the measures identified in AC-17.1.5.1 are being applied to enforce requirements for remote connections to the information system. |
| **AC-17.1.5.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with remote access control responsibilities; [*reviewing*] for further evidence that the measures identified in AC-17.1.5.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(1)** | REMOTE ACCESS |
| **AC-17(1).1**  **AC-17(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for remote access]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2  concurrent controls: AC-3, AC-4, AU-2, AU-3, AU-6, AU-7, AU-12, AU-14, CM-6, CM-8, IA-2,  IA-8, SC-7, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to facilitate the monitoring and control of remote access methods. |
| **AC-17(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-17(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-17(1).1.1.1. |
| **AC-17(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-17(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(2)** | REMOTE ACCESS |
| **AC-17(2).1**  **AC-17(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization uses cryptography to protect the confidentiality and integrity of remote access sessions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing cryptographic protections for remote access]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CM-6, IA-2, SC-7, SC-8, SC-9, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement cryptography to protect the confidentiality and integrity of remote access sessions. |
| **AC-17(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-17(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-17(2).1.1.1. |
| **AC-17(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-17(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(3)** | REMOTE ACCESS |
| **AC-17(3).1**  **AC-17(3).1.1**  **AC-17(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines a limited number of managed access control points for remote access to the information system; and* 2. *the information system routes all remote accesses through managed access control points.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for remote access]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-4, CM-6, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(3).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the managed access control points for remote access to the information system. |
|  |  |
| **AC-17(3).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to route all remote access through the managed access control points identified in AC-17(3).1.1.1. |
| **AC-17(3).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-17(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-17(3).1.2.1. |
| **AC-17(3).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-17(3).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(4)** | REMOTE ACCESS |
| **AC-17(4).1**  **AC-17(4).1.1**  **AC-17(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and* 2. *the organization documents the rationale for such access in the security plan for the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2  concurrent controls: AC-3, AC-4, AC-6, IA-2, MA-4, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(4).1.1.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the compelling operational needs to authorize remote access to privileged commands and security-relevant information. |
| **AC-17(4).1.1.2** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to authorize the execution of privileged commands and access to security-relevant information via remote access only for the compelling operational needs identified in AC-17(4).1.1.1. |
| **AC-17(4).1.1.3** | **Examine** authorization approvals for an agreed-upon [*basic*] sample of remote access accounts with access to privileged commands and security-relevant information; [*reviewing*] for evidence that the measures identified in AC-17(4).1.1.2 are being applied. |
| **AC-17(4).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with remote access authorization responsibilities; [*reviewing*] for further evidence that the measures identified in AC-17(4).1.1.2 are being applied. |
|  |  |
| **AC-17(4).1.2.1** | **Examine** security plan; [*reviewing*] for the rationale for the execution of privileged commands and access to security-relevant information via remote access. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(5)** | REMOTE ACCESS |
| **AC-17(5).1**  **AC-17(5).1.1**  **AC-17(5).1.2**  **AC-17(5).1.3**  **AC-17(5).1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of monitoring for unauthorized remote connections to the information system;* 2. *the organization monitors for unauthorized remote connections to the information system in accordance with the organization-defined frequency;* 3. *the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and* 4. *the organization takes organization-defined appropriate action(s) if an unauthorized connection is discovered.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for monitoring remote connections to the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AU-2, AU-3, AU-6, AU-7, AU-12, AU-14, CM-8, IA-8, SI-4, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(5).1.1.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the frequency of monitoring for unauthorized remote connections to the information system. |
|  |  |
| **AC-17(5).1.2.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to monitor for unauthorized remote access in accordance with the frequency identified in AC-17(5).1.1.1. |
| **AC-17(5).1.2.2** | **Examine** an agreed-upon [*basic*] sample of remote access monitoring records for the information system; [*reviewing*] for evidence that the measures identified in AC-17(5).1.2.1 are being applied to monitor for unauthorized remote access connections to the information system. |
| **AC-17(5).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for monitoring remote connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-17(5).1.2.1 are being applied. |
|  |  |
| **AC-17(5).1.3.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the appropriate action(s) to be taken if an unauthorized connection is discovered. |
|  |  |
| **AC-17(5).1.4.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to take the appropriate actions identified in AC-17(5).1.3.1 if an unauthorized connection is discovered. |
| **AC-17(5).1.4.2** | **Examine** after-action reports for an agreed-upon [*basic*] sample of unauthorized connections discovered; [*reviewing*] for evidence that the measures identified in AC-17(5).1.4.1 are being applied. |
| **AC-17(5).1.4.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for monitoring remote connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-17(5).1.4.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(6)** | REMOTE ACCESS |
| **AC-17(6).1**  **AC-17(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for implementing or monitoring remote access to the information system; information system users with knowledge of information about remote access mechanisms]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-8, PL-4, PS-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(6).1.1.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure that users protect information about remote access mechanisms from unauthorized use and disclosure. |
| **AC-17(6).1.1.2** | **Examine** rules of behavior documentation, access agreements, or other relevant documents for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the measures identified in AC-17(6).1.1.1 are being applied to ensure that users protect information about remote access mechanisms from unauthorized use and disclosure. |
| **AC-17(6).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with knowledge of information about remote access mechanisms; [*reviewing*] for further evidence that the measures identified in AC-17(6).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(7)** | REMOTE ACCESS |
| **AC-17(7).1**  **AC-17(7).1.1**  **AC-17(7).1.2**  **AC-17(7).1.3**  **AC-17(7).1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security functions and security-relevant information that can be accessed using remote sessions;* 2. *the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;* 3. *the organization employs organization-defined additional security measures for remote sessions used to access organization-defined security functions and security-relevant information; and* 4. *the organization audits remote sessions for accessing organization-defined security functions and security-relevant information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for remote access]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-6, AU-2, AU-3, AU-6, AU-7, AU-12, AU-14, CM-6,  SC-7, SC-8, SC-9  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(7).1.1.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the security functions and security-relevant information that can be accessed using remote sessions. |
|  |  |
| **AC-17(7).1.2.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the additional security measures to be employed for remote sessions used to access the security functions and security-relevant information identified in AC-17(7).1.1.1. |
|  |  |
| **AC-17(7).1.3.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the additional security measures identified in AC-17(7).1.2.1. |
| **AC-17(7).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-17(7).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-17(7).1.3.1. |
| **AC-17(7).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-17(7).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-17(7).1.4.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to audit remote sessions for accessing the security functions and security-relevant functions identified in AC-17(7).1.1.1. |
| **AC-17(7).1.4.2** | **Examine** audit records for an agreed-upon [*basic*] sample of remote sessions accessing the security functions and security-relevant information identified in AC-17(7).1.1.1; [*reviewing*] for evidence that the measures identified in AC-17(7).1.4.1 are being applied. |
| **AC-17(7).1.4.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for auditing remote access sessions; [*reviewing*] for further evidence that the measures identified in AC-17(7).1.4.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-17(8)** | REMOTE ACCESS |
| **AC-17(8).1**  **AC-17(8).1.1**  **AC-17(8).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the networking protocols within the information system deemed to be nonsecure; and* 2. *the organization disables the organization-defined networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; security plan; list of networking protocols deemed to be non-secure; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms disabling networking protocols deemed to be non-secure]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, CM-8, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-17(8).1.1.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the networking protocols within the information system deemed to be non-secure. |
|  |  |
| **AC-17(8).1.2.1** | **Examine** access control policy, procedures addressing remote access to the information system, security plan, or other relevant documents; [*reviewing*] for the explicit components that support specific operational requirements. |
| **AC-17(8).1.2.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to disable the networking protocols identified in AC-17(8).1.1.1 deemed to be non-secure except for the explicit components identified in AC-17(8).1.2.1. |
| **AC-17(8).1.2.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-17(8).1.2.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-17(8).1.2.2. |
| **AC-17(8).1.2.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-17(8).1.2.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |