# Procedure

The Security Checklist establishes the security controls to be monitored, the frequency of monitoring (weekly, monthly, quarterly, or annually), the criteria or evidence required to validate effectiveness of controls, and the process for proper handling of any deficiencies identified. [CA.L2-3.12.3, AU.L2-3.3.3]

**Security Checklist procedure:**

* 1. Each security control or event to be monitored is identified, and the general criteria/procedure for each, IAW AU.L2-3.3.3, CA.L2-3.12.3, CA.L2-3.12.2. Various evidence may be accepted providing they demonstrate compliance.

1. Action items such as patches needed, object cleanup, EDR agents missing, are noted for tracking but are not deficiencies.
2. **The IT Manager** reviews evidence, comments on any follow-up needed, and files the Security Checklist when completed.
3. **The IT Manager identifies, and tracks deficiencies as follows:**
   1. Before closing out each review, the IT Manager notes any deficiencies in the ‘Deficiency Tracking’ section.
   2. Definition: Deficiency is a temporary or permanent weakness or absence in the design, implementation, or operation of a security control that could prevent the organization from meeting its security objectives, protecting CUI, or adhering to CMMC requirements.
   3. Create a ticket and remediate within 30 days; Add to the Operational POA&M if more than 30 days is needed to properly address the deficiency.

# Schedule Tracking

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Code | Indicates | Weekly | Monthly | Quarterly | Annual |
| C | Completed on Time | Mon-Fri | By EOM | Within 7 days of EOQ | Within calendar year |
| M | Missed | Any later | Any later | Any later | Any later |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| 1st Quarter | **JAN >** | N/A | **FEB >** | N/A | **MAR >** | N/A |
| N/A | 1-7 > | N/A | 1-7 > | N/A | 1-7 > | N/A |
|  | 8-14 > | N/A | 8-14 > | N/A | 8-14 > | N/A |
|  | 15-21 > | N/A | 15-21 > | N/A | 15-21 > | N/A |
|  | 22-30 > | N/A | 22-30 > | N/A | 22-30 > | N/A |
|  |  |  |  |  |  |  |
| 2nd Quarter | **APRIL >** | N/A | **MAY >** | N/A | **JUNE >** | C |
| C | 1-7 > | N/A | 1-7 > | N/A | 1-7 > | C |
|  | 8-14 > | N/A | 8-14 > | N/A | 8-14 > | M |
|  | 15-21 > | N/A | 15-21 > | N/A | 15-21 > | C |
|  | 22-30 > | N/A | 22-30 > | N/A | 22-30 > | C |
|  |  |  |  |  |  |  |
| 3rd Quarter | **JULY >** | C | **AUG >** |  | **SEP >** |  |
|  | 1-7 > | C | 1-7 > | M | 1-7 > | C |
|  | 8-14 > | C | 8-14 > | C | 8-14 > | C |
|  | 15-21 > | C | 15-21 > | C | 15-21 > | C |
|  | 22-30 > | C | 22-30 > | C | 22-30 > |  |
|  |  |  |  |  |  |  |
| 4th Quarter | 0CT > |  | NOV > |  | DEC > |  |
|  | 1-7 > |  | 1-7 > |  | 1-7 > |  |
|  | 8-14 > |  | 8-14 > |  | 8-14 > |  |
|  | 15-21 > |  | 15-21 > |  | 15-21 > |  |
|  | 22-30 > |  | 22-30 > |  | 22-30 > |  |

# Deficiency Tracking

|  |
| --- |
| **Procedure**: The IT Manager identifies deficiencies and documents them in this section. At the end of each calendar year, a new empty Security Checklist is started and any deficiencies which have been closed out are removed from this list. Any deficiencies or issues identified are tracked via a ticket and may be also tracked on the Operational POA&M or the Risk Log as deemed necessary by the IT Manager to track the issue appropriately. [CA.L2-3.12.3, AU.L2-3.3.3, CA.L2-3.12.2] |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Control# | Date Identified | Ticket Number | Deficiency | Date Mitigated or Remediated | POAM/RL  (30+ days) |
| none | n/a | n/a | No deficiencies identified | n/a | n/a |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Weekly Checklist

## AC.L2-3.1.12 Remote Access Logs

|  |
| --- |
| **Procedure**: Review all instances of remote access in Entra ID Sign-in Logs:   1. Download the Entra > Monitoring and Health > Log Analytics > Queries > KH Remote Admin Weekly Audit 2. **IT Manager Review: N**ote any suspicious or unexpected logins, high numbers of failed logins. |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Initials | Ticket# | Note |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## MP.L2-3.8.9 | Backup Job Results

|  |  |  |  |
| --- | --- | --- | --- |
| **Procedure**: Insert screenshots of last 5 days of notifications for this job. | | | |
| Date | Initials | Ticket# | Note |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Monthly Checklist

## IA.L2-3.5.3 | VPN MFA |

|  |
| --- |
| Procedure: In AD, provide evidence of users authorized to access VPN   * Risky Users * Risky Sign-ins   Create ticket for any risk detections found and what was done in response. For example if risk detection was found to be false alarm, it can be marked as resolved in Entra and noted here, or a ticket could be created for IT manager to provide guidance, etc. |

## SI.L2-3.14.7 | Risky Users & Risky Logins |

|  |
| --- |
| Procedure: In Entra ID, go to Protection and then get screenshots of any risky logins.   * Risky Users * Risky Sign-ins   Create ticket for any risk detections found and what was done in response. For example if risk detection was found to be false alarm, it can be marked as resolved in Entra and noted here, or a ticket could be created for IT manager to provide guidance, etc. |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Initials | Ticket# | Note |
|  |  |  |  |
|  |  |  |  |

## IA.L2-3.5.3| Audit item 1

## IA.L2-3.5.3| Audit item 2

## IA.L2-3.5.3| Audit item 3