# Checklist for CSAF documents

This document shall provide a checklist for CSAF documents with respect to the different profiles. Please always use the checks for CSAF Base and in case another profile is used, please do the additional, specific checks.

For each profile a list of fields is provided that are considered best practice and should be filled. The mandatory fields that need to be provided are checked by schema validation.

## Checks for Profile CSAF Base

- Would a more specific profile better fit the purpose of this advisory?
- Are validation and document tests successful?
- Does the filename follow the specified rules (see section 5.1 of the specification)?
- Were all optional and informative tests executed and the results evaluated?

### Best Practice Fields to Check

- `/document/notes[]/title`
- `/vulnerabilities[]/scores[]/cvss_v3`
- `/vulnerabilities[]/scores[]/cvss_v3/attackComplexity`
- `/vulnerabilities[]/scores[]/cvss_v3/attackVector`
- `/vulnerabilities[]/scores[]/cvss_v3/availabilityImpact`
- `/vulnerabilities[]/scores[]/cvss_v3/confidentialityImpact`
- `/vulnerabilities[]/scores[]/cvss_v3/integrityImpact`
- `/vulnerabilities[]/scores[]/cvss_v3/privilegesRequired`
- `/vulnerabilities[]/scores[]/cvss_v3/scope`
- `/vulnerabilities[]/scores[]/cvss_v3/userInteraction`

## Checks for Profile CSAF Security Incident Response

- Is the `/document/category` set to `csaf_security_incident_response`?
- Is there a reasonable description to understand the response on the incident (`/document/notes`)?

### Best Practice Fields to Check

- `/document/distribution`
- `/document/notes[]/title`
- `/vulnerabilities[]/scores[]/cvss_v3`
- `/vulnerabilities[]/scores[]/cvss_v3/attackComplexity`
- `/vulnerabilities[]/scores[]/cvss_v3/attackVector`
- `/vulnerabilities[]/scores[]/cvss_v3/availabilityImpact`
- `/vulnerabilities[]/scores[]/cvss_v3/confidentialityImpact`
- `/vulnerabilities[]/scores[]/cvss_v3/integrityImpact`

- /vulnerabilities[]/scores[]/cvss_v3/privilegesRequired
- /vulnerabilities[]/scores[]/cvss_v3/scope
- /vulnerabilities[]/scores[]/cvss_v3/userInteraction

## Checks for Profile CSAF Informational Advisory

- Is the /document/category set to csaf_informational_advisory?
- Is there a reasonable description to understand the real problem and the recommendations on the incident (/document/notes)?

### Best Practice Fields to Check

Best Practice Fields

- /document/distribution
- /document/notes[]/title

## Checks for Profile CSAF Security Advisory

- Is the /document/category set to csaf_security_advisory?
- In case of mainly listing not affected products, please use profile VEX.
- Are all products described properly and well identifiable (/vulnerabilities[]/product_status)?
- Are all remediations for affected products described properly and understandable, i.e. is there an action statement in /vulnerabilities[]/remediations?

### Best Practice Fields to Check

- /document/acknowledgments
- /document/acknowledgments[]/names
- /document/acknowledgments[]/organization
- /document/acknowledgments[]/summary
- /document/aggregate_severity/text
- /document/distribution
- /document/distribution/tlp
- /document/distribution/tlp/label
- /document/notes
- /document/notes[]/title
- /document/publisher/contact_details
- /document/references
- /product_tree/branches
- /vulnerabilities[]/acknowledgments[]/names
- /vulnerabilities[]/acknowledgments[]/organization
- /vulnerabilities[]/acknowledgments[]/summary
- /vulnerabilities[]/cve

- /vulnerabilities[]/cwe
- /vulnerabilities[]/involvements[]/date
- /vulnerabilities[]/involvements[]/summary
- /vulnerabilities[]/notes[]/title
- /vulnerabilities[]/product_status/fixed
- /vulnerabilities[]/product_status/known_affected
- /vulnerabilities[]/references
- /vulnerabilities[]/remediations
- /vulnerabilities[]/remediations[]/url
- /vulnerabilities[]/scores
- /vulnerabilities[]/scores[]/cvss_v3
- /vulnerabilities[]/scores[]/cvss_v3/attackComplexity
- /vulnerabilities[]/scores[]/cvss_v3/attackVector
- /vulnerabilities[]/scores[]/cvss_v3/availabilityImpact
- /vulnerabilities[]/scores[]/cvss_v3/confidentialityImpact
- /vulnerabilities[]/scores[]/cvss_v3/integrityImpact
- /vulnerabilities[]/scores[]/cvss_v3/privilegesRequired
- /vulnerabilities[]/scores[]/cvss_v3/scope
- /vulnerabilities[]/scores[]/cvss_v3/userInteraction
- /vulnerabilities[]/threats[]/date
- /vulnerabilities[]/threats[]/group_ids
- /vulnerabilities[]/threats[]/product_ids
- /vulnerabilities[]/title

## Checks for Profile CSAF VEX

- Is the `/document/category` set to `csaf_vex`?
- Are all remediations for affected products described properly and understandable, i.e. is there an action statement in `/vulnerabilities[]/remediations`?
- For not affected products, there must be a reasonable description to show why the product is not affected (impact statement).

### Best Practice Fields to Check

- /document/notes[]/title
- /document/publisher/contact_details
- /document/references
- /product_tree/branches
- /vulnerabilities[]/flags[]/date
- /vulnerabilities[]/involvements[]/date
- /vulnerabilities[]/involvements[]/summary
- /vulnerabilities[]/notes[]/title

- /vulnerabilities[]/references
- /vulnerabilities[]/remediations[]/url
- /vulnerabilities[]/scores[]/cvss_v3
- /vulnerabilities[]/scores[]/cvss_v3/attackComplexity
- /vulnerabilities[]/scores[]/cvss_v3/attackVector
- /vulnerabilities[]/scores[]/cvss_v3/availabilityImpact
- /vulnerabilities[]/scores[]/cvss_v3/confidentialityImpact
- /vulnerabilities[]/scores[]/cvss_v3/integrityImpact
- /vulnerabilities[]/scores[]/cvss_v3/privilegesRequired
- /vulnerabilities[]/scores[]/cvss_v3/scope
- /vulnerabilities[]/scores[]/cvss_v3/userInteraction
- /vulnerabilities[]/threats[]/date