Software Review and Risk Assessment Process

✅ *How to Use This Form*

Gather Initial Ticket Info:

- Fill out **Section 1** (Request Information) and **Section 2** (software details).
- Use the sandbox if compatible with CrowdStrike or related tools; otherwise, request an SBOM.
- If file size or format is too large or unsupported, proceed with SBOM analysis.

Sandbox or SBOM:

- If sandbox testing is possible, upload the file into either VT or CS and save the full report for your sandbox of choice. Record findings in **Section 3** under “Sandbox Observations.”
- If sandboxing isn’t feasible, document **SBOM** findings in **Section 4**.

Malware & Suspicious Activity:

- Use **Section 5 & 6** to document indicators from antivirus, EDR, or other threat intelligence sources for tracking malicious alerts.

Rate the Risk:

- In **Section 7**, combine vulnerability analysis and malicious indicators for an overall risk rating (High/Medium/Low or numeric scale).

Mitigate & Recommend:

- In **Section 8**, outline specific remediation steps or required compensating controls (e.g., patch, upgrade, restrict network access).

Final Decision:

- In **Section 9**, specify whether to **approve, approve with conditions, or deny** the request to standardize software clearance.

Formal Sign-Off:

- **Section 10** records the final sign-off from both the reviewing security team and the relevant management or approval authority.

Category	Details
1. **Request Information**	
Requestor	[Name/Dept/Contact]
Ticket/Case ID	[ID]
Request Date	[Date]
Reviewer(s)	[Name / Team]
2. **Software Details**	
Software Name	[Product Name]
Version	[Version Number]
Vendor / Publisher	[Vendor]
Purpose / Business Use Case	[Summary of the software’s function]
Deployment Environment	[Endpoint, Server, Cloud, etc.]
File Size (if relevant)	[Approximate MB/GB]

Why Sandbox Not Used (if applicable)	[e.g., File too large, vendor format incompatible, etc.]
3. **Review Method**	
Sandboxing Performed?	[Yes/No]
If Yes, Sandbox Observations	[List any behaviors observed, file modifications, network calls, etc.]
If No, SBOM-Based Review	[Proceed with the SBOM analysis details below.]
4. **SBOM Analysis (if applicable)**	
SBOM Provided (Y/N)	[Yes/No]
SBOM Format	[SPDX, CycloneDX, etc.]
SBOM File Name/Location	[Link or Attachment]
Date of SBOM	[When was it generated?]
SBOM Components	
Total Components	[Count]
Third-Party Libraries	[List or count key ones]
Open Source Components	[List or count key ones]
Proprietary Components	[List or count key ones]
5. **Vulnerability Scan**	
Tool(s) Used	[e.g., SCA tool, vulnerability scanner, etc.]
Known Vulnerabilities	
1. Component	[Name & Version]
• CVE(s)	[CVE-XXXX-XXXX, etc.]
• Severity	[CVSS Score / High/Medium/Low]
• Patch Available	[Yes/No]
2. ...	
Action Taken or Required	[Check vendor advisories, patch, upgrade?]
6. **Malicious or Suspicious Findings**	
Malicious Indicators	
List any detections	[List any detections from AV, EDR, or threat intel feeds]
File Hash	[MD5/SHA-256]
Detection Name	[Trojan, Adware, etc.]
Source of Alert	[AV product, SIEM, IDS, etc.]
Vendor Statement	[If vendor acknowledges or denies the detection, mentions false positives, etc.]

Behavioral Analysis	[If partial sandbox or other dynamic analysis was performed, note suspicious behaviors—file modifications, registry changes, outbound connections, etc.]
7. **Risk Assessment**	
Overall Risk Rating	[High / Medium / Low / Unknown]
Justification	[Key reasons for rating: severity/volume of vulnerabilities, malicious flags, exploit maturity, vendor track record, environment sensitivity, etc.]
8. **Mitigations & Recommendations**	
Required Remediation	
• `1`	[Patch / update specific components]
• `1`	[Workarounds or configuration changes]
• `1`	[Isolate or limit privileges for this software]
Additional Controls	
• `1`	[E.g., network segmentation, continuous monitoring, restricted environment, vendor SLA for security fixes, etc.]
9. **Decision & Approval**	
Decision	[Approved / Approved w/Conditions / Denied]
Rationale	[Brief explanation of final decision]
Conditions (if any)	[Conditions for approval, e.g., restrict to test environment, mandatory quarterly updates, etc.]
10. **Sign-Off**	
Security Team/Reviewer	[Name / Title / Signature / Date]
Management Approval	[Name / Title / Signature / Date]