

**FOR MORE INFORMATION  
SCAN THE QR CODE**

***“Never travel the  
Information Super Highway  
without the Software  
Assurance Guardian Point  
Man™(SAG-PM™) by your  
side to detect cyber risks and  
help you look both ways  
before installing software in  
production environments.”***

***“Trust is both a glue and a  
lubricant, holding society  
together and allowing its  
many parts to move  
smoothly. If trust can’t be  
made suitable for the digital  
age, the digital age won’t  
function.”“  
World Economic Forum  
Davos 2021***



**BUSINESS CYBER GUARDIAN™  
23 LINDA DRIVE  
WESTFIELD, MA 01085**

**PHONE: +1 978-696-1788**

***Risk always exists, but trust  
must be earned and awarded.***

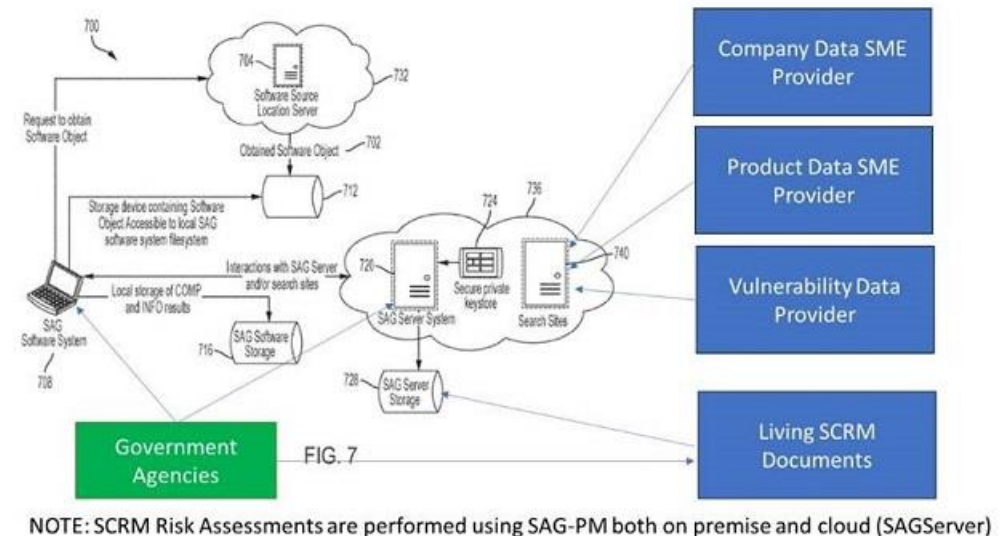
***Never Trust Software, always  
verify and report!™***



## About Business Cyber Guardian™

Business Cyber Guardian™ (BCG) is a software engineering company located in Westfield, MA providing software and services to help businesses implement Cyber Risk Management best practices and detect cyber risks, such as CISA KEVs, in software supply chains before buying or installing a software product and verify trustworthy software products adhering to CISA ["Secure by Design" principles](#) following the August 1, 2024 release of the [CISA Software Acquisition Guide](#)

## High Level Implementation Model



1. Perform introspection and process SBOM data
2. Verify Download Server Source Location/Certificate
3. Perform Virus Scan
4. Verify Digital Signature of software object
5. Perform CISA KEV detection and Vulnerability (CVE) Search using NIST NVD and Vendor supplied Attestation data (SBOM VDR)
6. Perform Vendor Verification using Attestation data
7. Perform Provenance Check
8. Generate SAGScore™ (Trustworthiness Score)
9. Generate Risk Assessment and Detection Evidence Data
10. Save evidence in a tamper-proof form
11. IF a cyber risk is detected:
  1. Notify management immediately
  2. Discuss materiality and decide if a Form 8-K is required, under the protection of Client-Attorney privilege
  3. File a Form 8-K if required, within four business days of determining materiality of the cyber-risk/incident