# Example Corp Software Bill of Material (SBOM) Requirements FAQ

## Overview

1. How can SBOMs be generated and maintained?

At Example Corp, SBOMs must be generated and maintained for both 3rd party and internal software. This requirement is true for both COTS and SaaS software vendors. Per the requirements of their contact all vendors must provide an SBOM at the time of delivery with any software delivery, patch, or update. Exceptions to this policy must be approved by the legal department ([legal@example.com](mailto:legal@example.com)). Failure to deliver SBOMs in a timely manner will be considered cause for early contract termination. For any issues with timeliness of delivery please forward them to the Slack group #sboms or contact Carlos Salazar directly.

Internal products developed at Example Corp must comply with all security policies for SBOMs, including delivery of SBOMs prior to pushing to production. Any breach of this policy requires an exemption from AppSec or will be considered a Sev1 security issue.

2. Where do I store SBOMs data files?

At Example Corp, SBOMs must be stored in a secure, centralized repository with access controls and audit logging capabilities. The ESSS (Example SBOM storage system) should be used for storage. All deployments are required to include SBOM publishing to ESSS prior to moving from the SIT to UAT environments. Any breach of this policy requires an exemption from AppSec or will be considered a Sev1 security issue.

3. What do for SBOMs for SaaS and or managed services?

At Example Corp, SBOMs are required for all services used, however certain managed service providers, such as those from AnyCompany Cloud Services, have auxiliary agreements in place that changes this requirement. For any questions on if a specific SaaS or managed service requires an SBOM please contact AppSec, the legal department (legal@example.com) , and Carlos Salazar to obtain clarification and any approved exception required.