Qualcomm

NIST Working Group Voluntary Reporting Approach

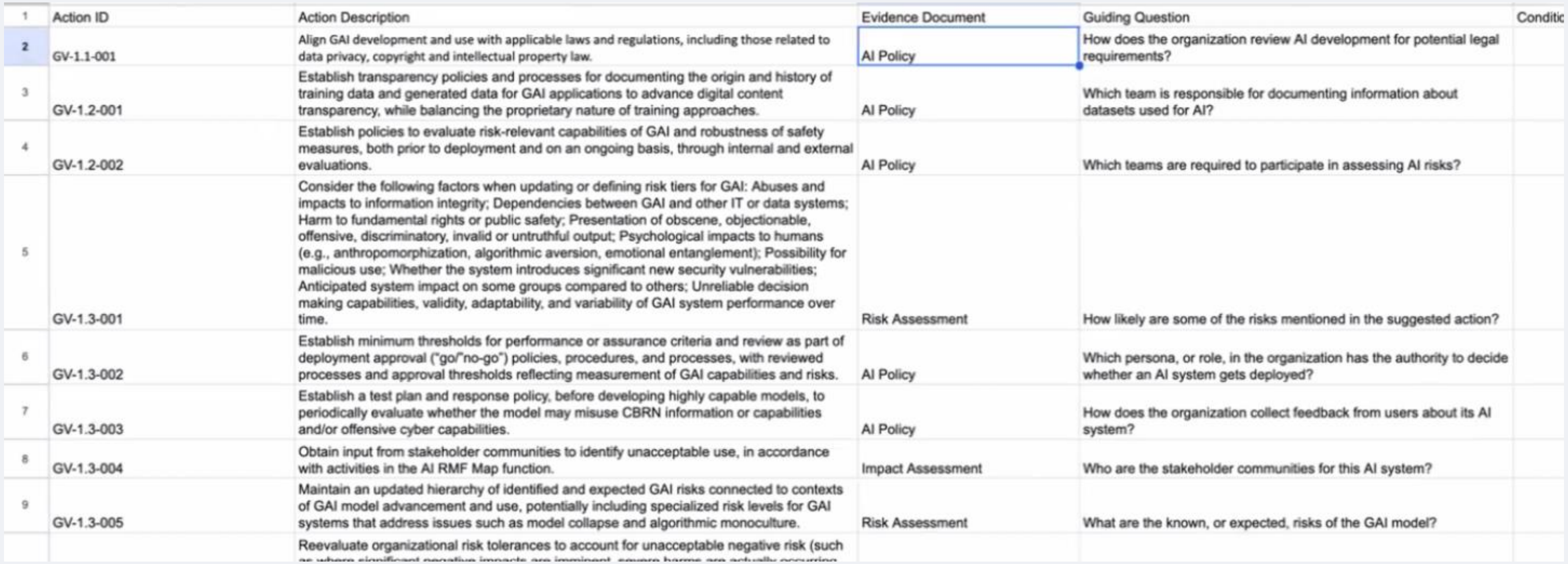
Laurie Grant

Sr. Director, Project Management
Qualcomm Technologies, Inc.

October 2024

Voluntary Reporting Approach

- Establish a consortium to launch and maintain mechanisms for voluntary reporting
- Create a companion website for conformance declaration, helpful information, and related tools
- Map NIST RAI Framework to a basic set of evidence documents (see Trustible example below)
- Design a macro-level reporting checklist at the evidence document level
- Drive and align with ISO and other related standards e.g., CEN-CENELEC
- Consider expanding to cover AI laws and regulations broadly with a consolidated effort and common solution
- Consider OpenChain as a reference framework for this type of capability (link and examples follow)



1	Action ID	Action Description	Evidence Document	Guiding Question	Conditic
2	GV-1.1-001	Align GAI development and use with applicable laws and regulations, including those related to data privacy, copyright and intellectual property law.	AI Policy	How does the organization review AI development for potential legal requirements?	
3	GV-1.2-001	Establish transparency policies and processes for documenting the origin and history of training data and generated data for GAI applications to advance digital content transparency, while balancing the proprietary nature of training approaches.	AI Policy	Which team is responsible for documenting information about datasets used for AI?	
4	GV-1.2-002	Establish policies to evaluate risk-relevant capabilities of GAI and robustness of safety measures, both prior to deployment and on an ongoing basis, through internal and external evaluations.	AI Policy	Which teams are required to participate in assessing AI risks?	
5	GV-1.3-001	Consider the following factors when updating or defining risk tiers for GAI: Abuses and impacts to information integrity; Dependencies between GAI and other IT or data systems; Harm to fundamental rights or public safety; Presentation of obscene, objectionable, offensive, discriminatory, invalid or untruthful output; Psychological impacts to humans (e.g., anthropomorphization, algorithmic aversion, emotional entanglement); Possibility for malicious use; Whether the system introduces significant new security vulnerabilities; Anticipated system impact on some groups compared to others; Unreliable decision making capabilities, validity, adaptability, and variability of GAI system performance over time.	Risk Assessment	How likely are some of the risks mentioned in the suggested action?	
6	GV-1.3-002	Establish minimum thresholds for performance or assurance criteria and review as part of deployment approval ("go/"no-go") policies, procedures, and processes, with reviewed processes and approval thresholds reflecting measurement of GAI capabilities and risks.	AI Policy	Which persona, or role, in the organization has the authority to decide whether an AI system gets deployed?	
7	GV-1.3-003	Establish a test plan and response policy, before developing highly capable models, to periodically evaluate whether the model may misuse CBRN information or capabilities and/or offensive cyber capabilities.	AI Policy	How does the organization collect feedback from users about its AI system?	
8	GV-1.3-004	Obtain input from stakeholder communities to identify unacceptable use, in accordance with activities in the AI RMF Map function.	Impact Assessment	Who are the stakeholder communities for this AI system?	
9	GV-1.3-005	Maintain an updated hierarchy of identified and expected GAI risks connected to contexts of GAI model advancement and use, potentially including specialized risk levels for GAI systems that address issues such as model collapse and algorithmic monoculture.	Risk Assessment	What are the known, or expected, risks of the GAI model?	
		Reevaluate organizational risk tolerances to account for unacceptable negative risk (such			

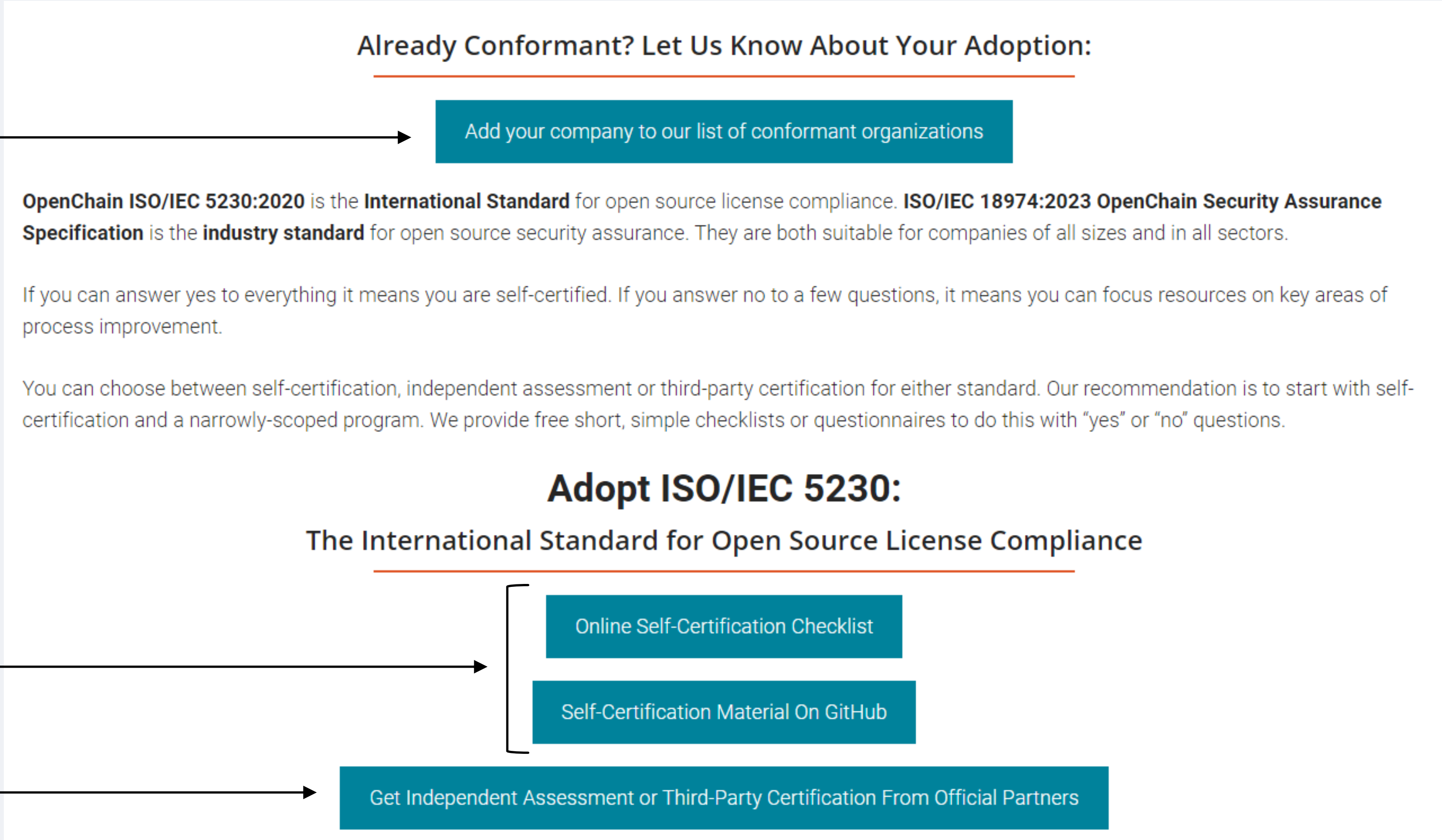
OPENCHAIN Reference Implementation

https://openchainproject.org/get-started

Self-Declare Conformance

Self-Certification Checklist & Materials

Assessment & Certification Partners



Already Conformant? Let Us Know About Your Adoption:

OpenChain ISO/IEC 5230:2020 is the **International Standard** for open source license compliance. **ISO/IEC 18974:2023 OpenChain Security Assurance Specification** is the **industry standard** for open source security assurance. They are both suitable for companies of all sizes and in all sectors.

If you can answer yes to everything it means you are self-certified. If you answer no to a few questions, it means you can focus resources on key areas of process improvement.

You can choose between self-certification, independent assessment or third-party certification for either standard. Our recommendation is to start with self-certification and a narrowly-scoped program. We provide free short, simple checklists or questionnaires to do this with "yes" or "no" questions.

Adopt ISO/IEC 5230:

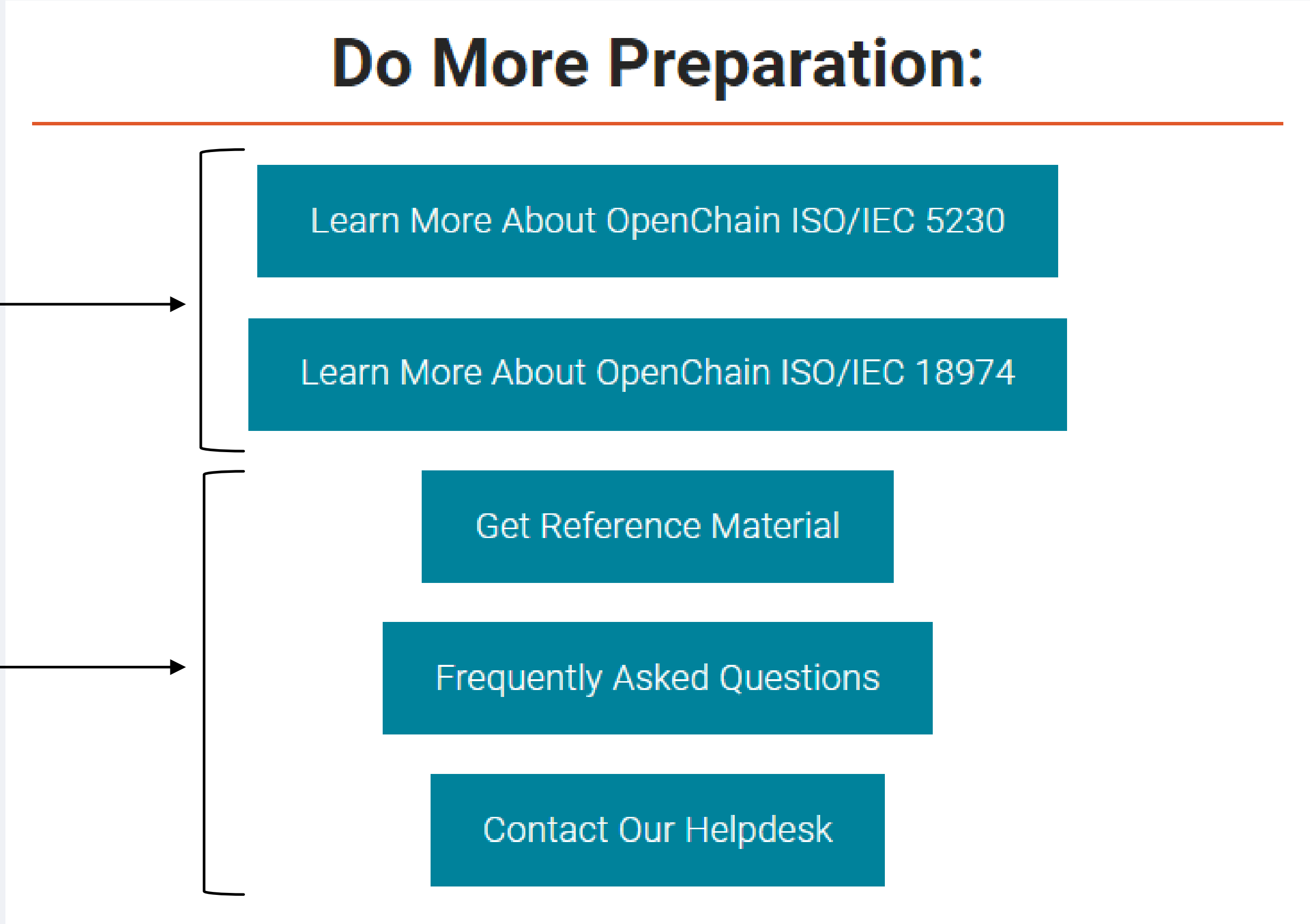
The International Standard for Open Source License Compliance

Online Self-Certification Checklist
Self-Certification Material On GitHub
Get Independent Assessment or Third-Party Certification From Official Partners

OPENCHAIN Reference Implementation, cont.

ISO/IEC Standards

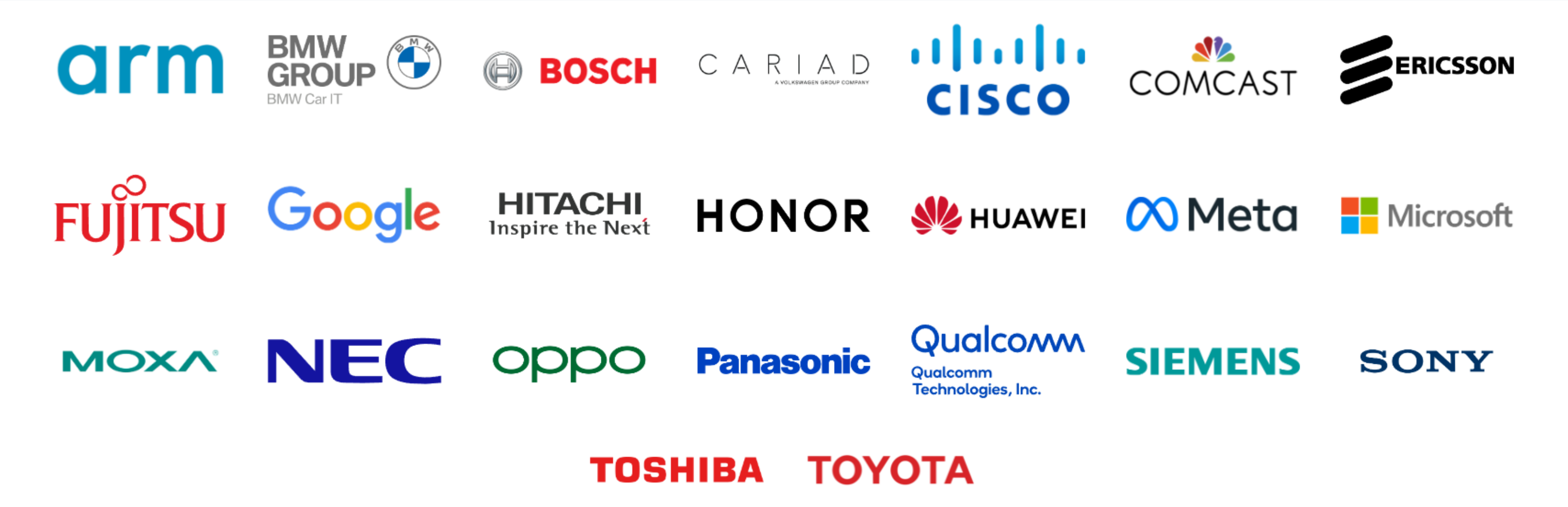
References & Help



Do More Preparation:

Learn More About OpenChain ISO/IEC 5230
Learn More About OpenChain ISO/IEC 18974
Get Reference Material
Frequently Asked Questions
Contact Our Helpdesk

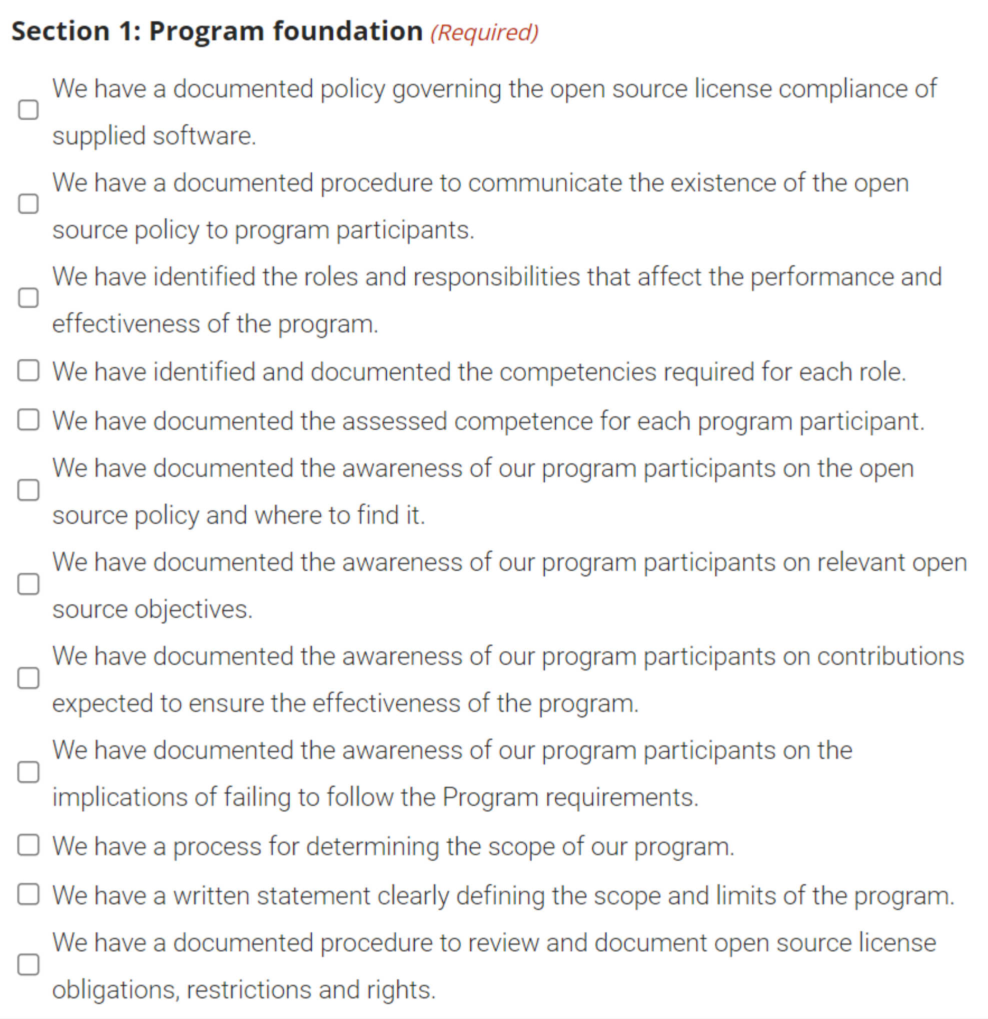
OPENCHAIN Platinum Members



OpenChain has PAS ISO submitter capability through the Joint Development Foundation and has authored specs e.g., ISO/IEC 5230:2020, and thereby has experience with open certification (self and third party enabled) processes.

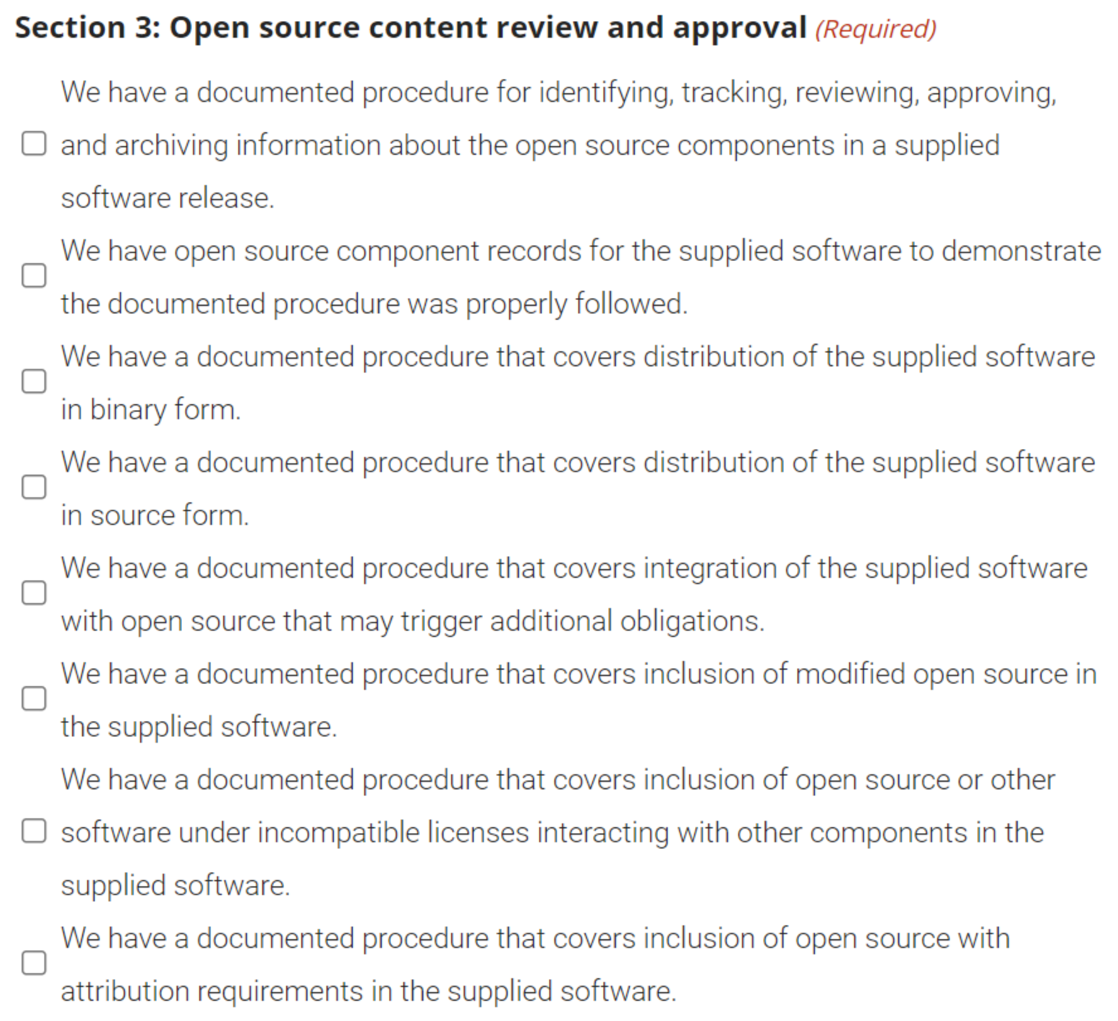
OPENCHAIN Conformance Checklist – Examples

Level of detail and structure of statements is illustrative and not intended to be a recommendation for an AI checklist



Section 1: Program foundation *(Required)*

- □ We have a documented policy governing the open source license compliance of supplied software.
- □ We have a documented procedure to communicate the existence of the open source policy to program participants.
- □ We have identified the roles and responsibilities that affect the performance and effectiveness of the program.
- □ We have identified and documented the competencies required for each role.
- □ We have documented the assessed competence for each program participant.
- □ We have documented the awareness of our program participants on the open source policy and where to find it.
- □ We have documented the awareness of our program participants on relevant open source objectives.
- □ We have documented the awareness of our program participants on contributions expected to ensure the effectiveness of the program.
- □ We have documented the awareness of our program participants on the implications of failing to follow the Program requirements.
- □ We have a process for determining the scope of our program.
- □ We have a written statement clearly defining the scope and limits of the program.
- □ We have a documented procedure to review and document open source license obligations, restrictions and rights.



Section 3: Open source content review and approval *(Required)*

- □ We have a documented procedure for identifying, tracking, reviewing, approving, and archiving information about the open source components in a supplied software release.
- □ We have open source component records for the supplied software to demonstrate the documented procedure was properly followed.
- □ We have a documented procedure that covers distribution of the supplied software in binary form.
- □ We have a documented procedure that covers distribution of the supplied software in source form.
- □ We have a documented procedure that covers integration of the supplied software with open source that may trigger additional obligations.
- □ We have a documented procedure that covers inclusion of modified open source in the supplied software.
- □ We have a documented procedure that covers inclusion of open source or other software under incompatible licenses interacting with other components in the supplied software.
- □ We have a documented procedure that covers inclusion of open source with attribution requirements in the supplied software.

Thank you

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

Qualcomm and Snapdragon are trademarks or registered trademarks of Qualcomm Incorporated.
Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.
Qualcomm patented technologies are licensed by Qualcomm Incorporated.

Follow us on: in 𝕏 ◎ ▶ f
For more information, visit us at qualcomm.com & qualcomm.com/blog