TOSHIBA

ISO/IEC 5230 Conformance:
Toshiba Case Study on Self-Certification

Takashi Ninjouji, Toshiba Corporation
Masaya Tarui, Toshiba Corporation

OpenChain Taiwan Workgroup meerting
August 26 2022

Contents and Speakers

01 Strategy for ISO/IEC 5230 Conformance

- **Takashi Ninjouji**
  Promoting Open Source, InnerSource and SPI
  OpenChain Project, OIN

02 Case Study

- **Masaya Tarui**
  Lead Software Architect, Cloud Computing Development
  Ruby Core Committer (2010-Current)

01

Strategy for ISO/IEC 5230 Conformance

Takashi Ninjouji

Chief Specialist
at Corporate Software Engineering Technology Center (SWC)

Work Experience

1998~	NTT	IPv6
2001~	DOCOMO	Mobile AR, HCI, Mobile Equipment (3G, 3.5G)
2011~	DeNA	Open Source Program, Mobile games
2020~	TOSHIBA	Promoting Open Source, InnerSource and SPI

Open Source

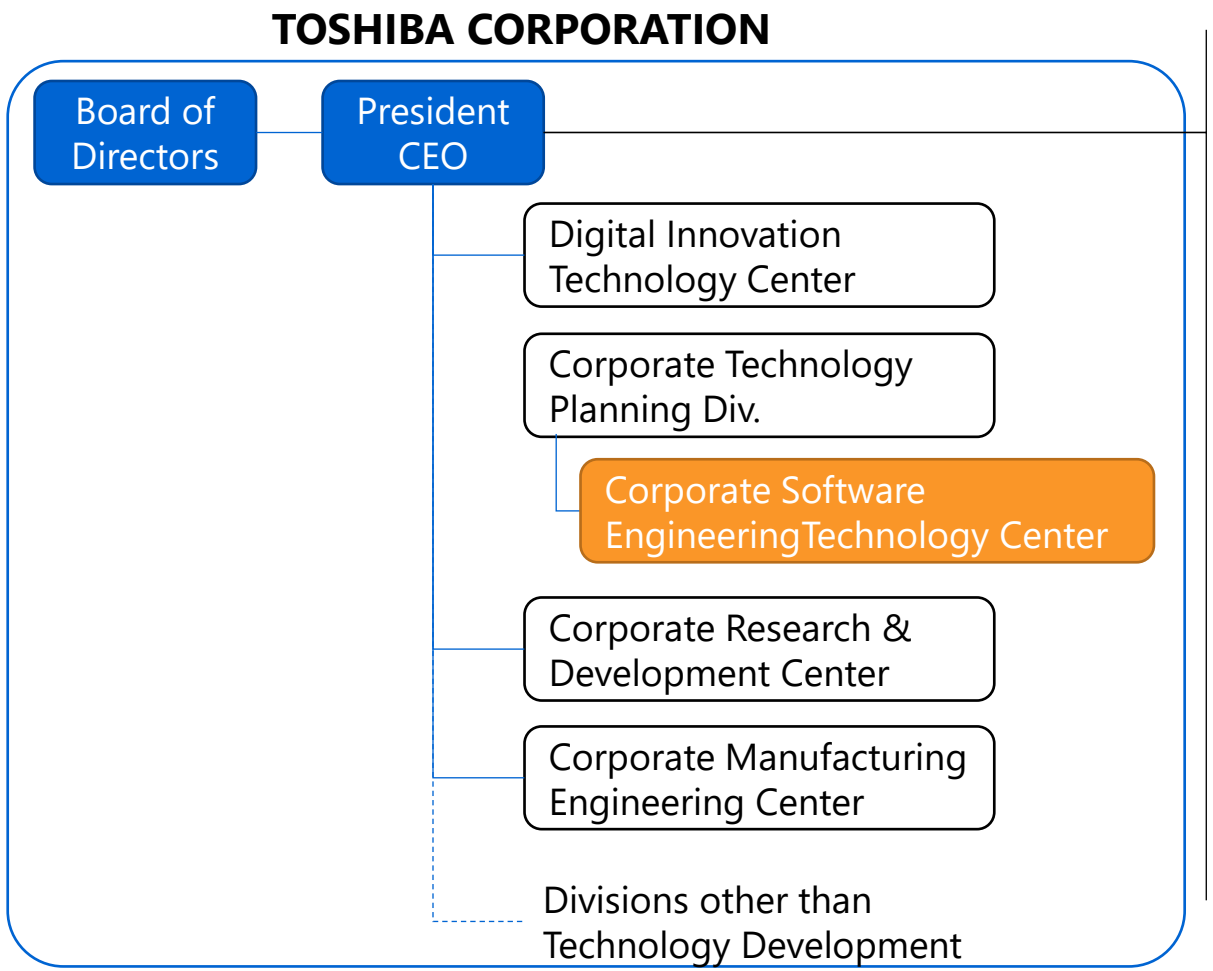
2018~	Community member of the OpenChain Project
2020~	Board member of the OpenChain Project (TOSHIBA)
	Technical Advisory Council of OIN (TOSHIBA)

*SPI: Software Process Improvement

Corporate Software Engineering Technology Center (SWC)

Mission

Standardization and deployment of Software Development Technologies



Energy Systems & Solutions
- Toshiba Energy System & Solutions Corporation
- Toshiba Plant Systems & Service Corporation

Infrastructure Systems & Solutions
- Toshiba Infrastructure Systems & Solution Corporation

Building Solutions
- Toshiba Elevator and Building Systems Corporation
- Toshiba Lighting & Technology Corporation
- Toshiba Carrier Corporation

Retail & Printing Solutions
- Toshiba Tec Corporation

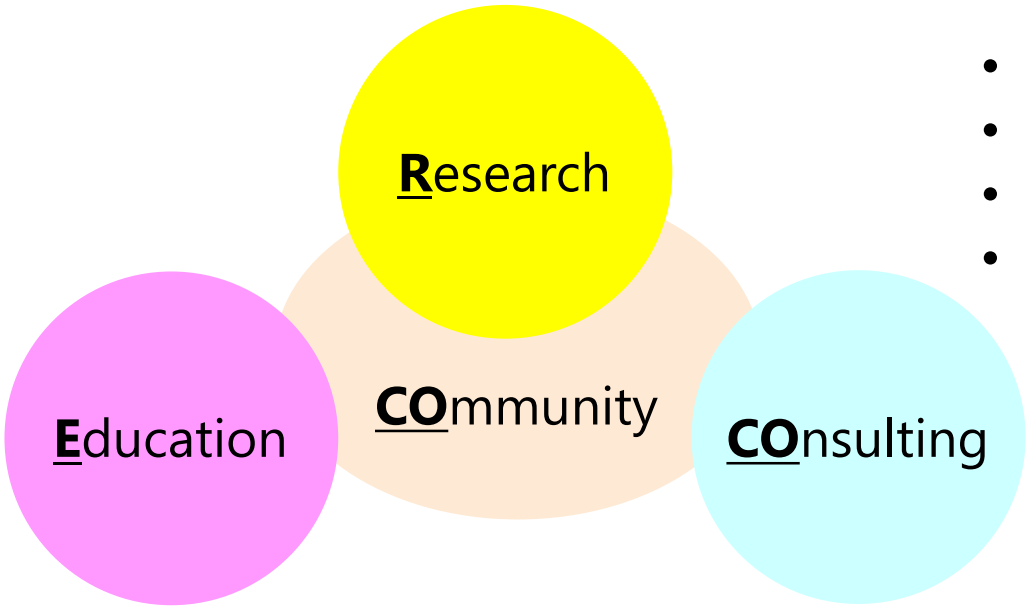
Electronic Device & Storage Solutions
- Toshiba Electronic Devices & Storage Corporation

Digital Solutions
- Toshiba Digital Solution Corporation

Software Process Improvement (SPI) in Toshiba

- **Group-wide efforts to Standardize and Improve Software Development Process**
  - Reference Process standards:
    CMMI, ITIL 4, ISO/IECs, etc. ← ISO/IEC 5230:2020
  - Introducing:
    Agile, DevOps, Microservice Architecture (MSA)

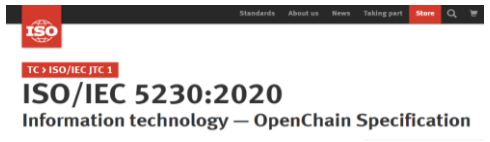
- **RECOCO model for In-house Engineering Support**



- R: Research (Technology to drive improvement)
- E: Education (Human resources development)
- CO : Consulting (Support SPI at development sites)
- CO : Communication (Community of Practice)

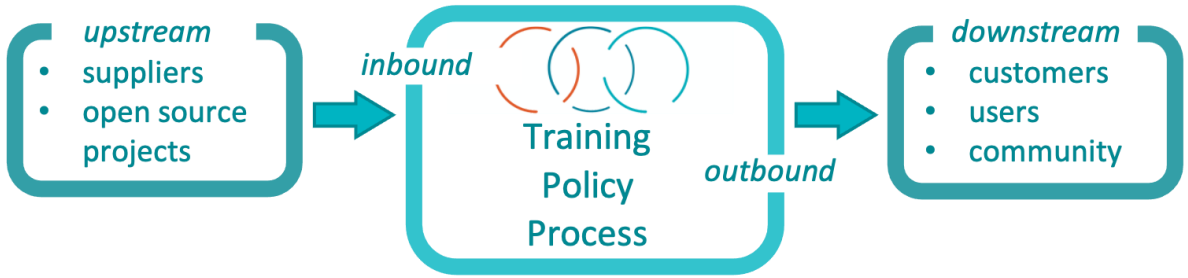
OpenChain Spec. 2.1 >> ISO/IEC 5230:2020

Building Trust In The Software Supply Chain with Open Source (Compliance) Program Standard



Functionally equivalent

OPENCHAIN (Specification 2.1/2.0)



Requirements
1. Program foundation
2. Relevant tasks defined and supported
3. Open source content review and approval
4. Compliance artifact creation and delivery
5. Understand open Source community engagement
6. Adherence to the Specification Requirements

- ✓ Program established
- ✓ Tasks defined
- ✓ Review and approval process
- ✓ Compliance artifacts collected
- ✓ Community engagement policy

Opinions observed (in OpenChain community)

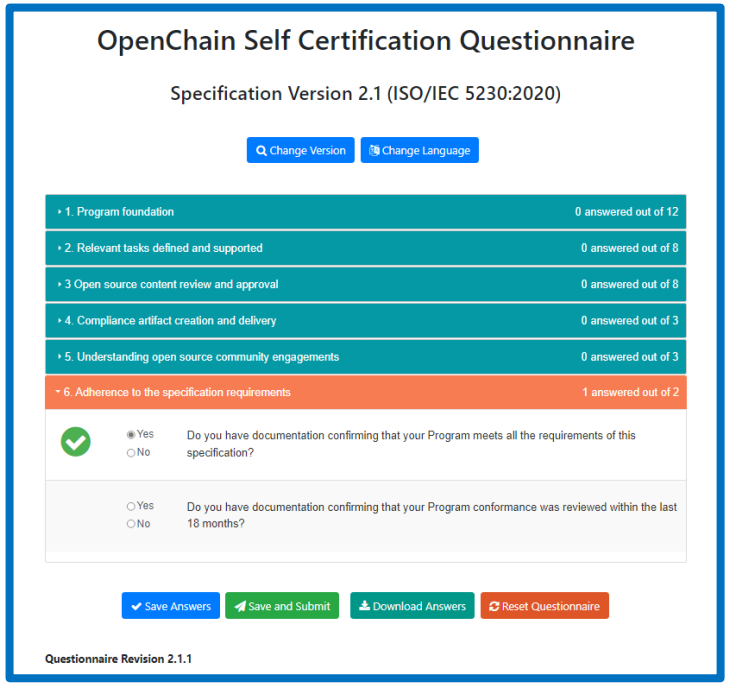
- Process implementation and evidence management contribute **to improve productivity and risk prevention (risk prediction)**
- It can be applied **to compliance for software of third-party origin**, including OSS
- **SBOM** management can be used as a **basis for vulnerability management**

Certification: Self or Third-Party

The treatment of conformance is the same.

Self-Certification

Answer on the OpenChain project website



Third-Party Certification

Certification by Partner

Certification: Self or Third-Party (cont'd)

OpenChain Specification's principle is "Less is More"

Self-Certification

Need to define the level of achievement

Considering the Specification, Questionnaires, and Trends in Open Source community and the market.

Third-Party Certification

No particular unified standard for third-party certification

e.g.
There is no such qualification as CMMI appraisal.

Certification: Self or Third-Party (cont'd)

Most of programs adopt **Self-Certification**.

Publicly Announced ISO/IEC 5230 Programs

2020/12/01	TOYOTA
2020/12/15	NCSOFT
2020/12/17	Cisco
2021/01/13	NTT Data
2021/02/01	Microsoft
2021/02/08	HITACHI
2021/03/02	LG
2021/04/06	Nanjing Fujitsu Nanda Software Technology Co., Ltd.
2021/04/22	Keitaro
2021/07/07	Samsung Electronics
2021/07/13	Bosch
2021/08/09	Sony Semiconductor
2021/08/19	QCT
2021/08/22	Coontec
2021/09/07	Woven Planet
2021/09/08	Synology
2021/09/08	SK Telecom
2021/10/19	NEC
2021/12/15	ETRI
2022/01/24	Kakaobank
2022/01/24	Kakao
2022/02/14	GBase 8a from General Data Technology Co., Ltd. (GBASE)
2022/02/14	KingbaseES V8 from CETC Kingbase
2022/02/14	Tidb enterprise v4.0 from PingCap
2022/03/17	BlackBerry
2022/03/28	Revenera
2022/03/28	SAP
2022/04/06	TOSHIBA

* Underlined: third-party certification

https://www.openchainproject.org/news

Strategy for conformance

Means: Self-Certification

Leverage the existing framework

- Organize and clarify rules and guidelines for smooth implementation

Localize the cost of

- **Developing Policy, Process, Rules, and related documents; and**
- **Coordinating with related departments**

Improvement Support Team and its Efforts

Team

- SPI Expert : Progress Management
- OSS (compliance) Expert : Open Source (License) Compliance, OpenChain Spec.

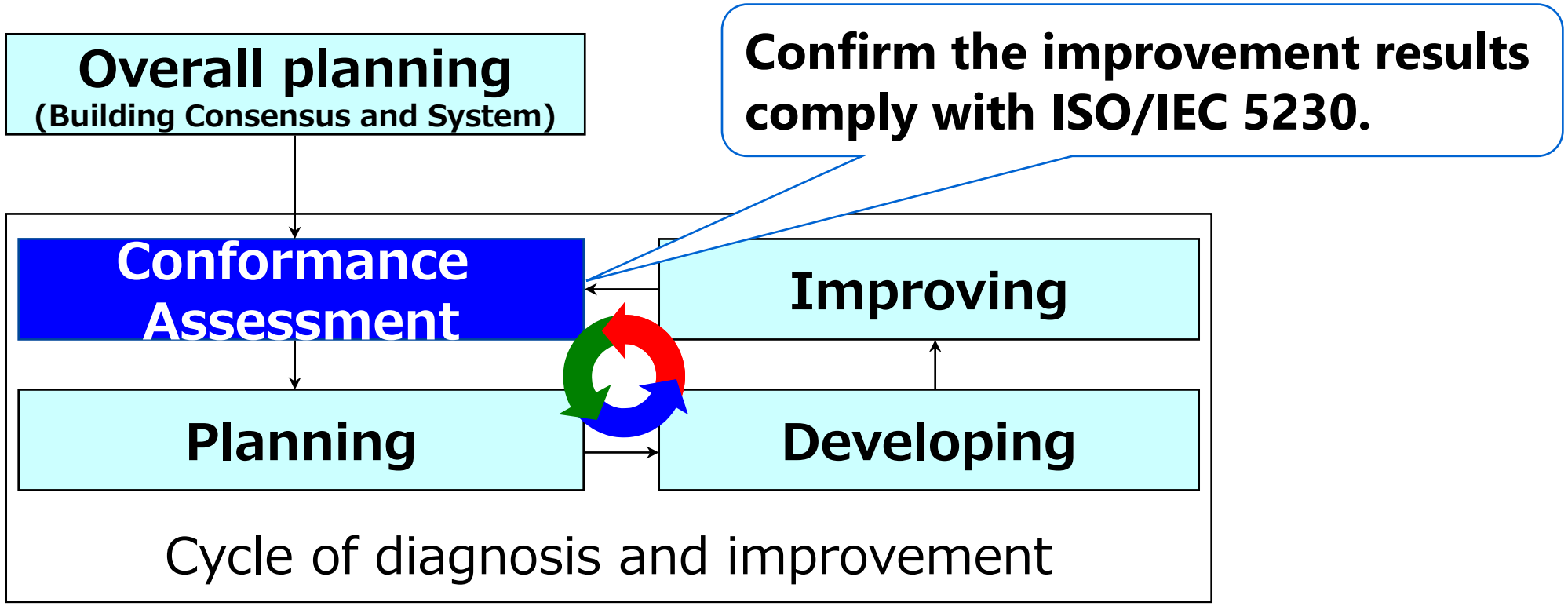
Efforts

- Clarify Interpretations of Specification and Questionnaires
- Clarify Conformance Criteria
- Template
  - Policy, Process, Competence, and more
  - Customizable for ISO/IEC 5230 compliance
- E-learning materials
- Interview Sheet

Purpose of ISO/IEC 5230 Conformance Assessment

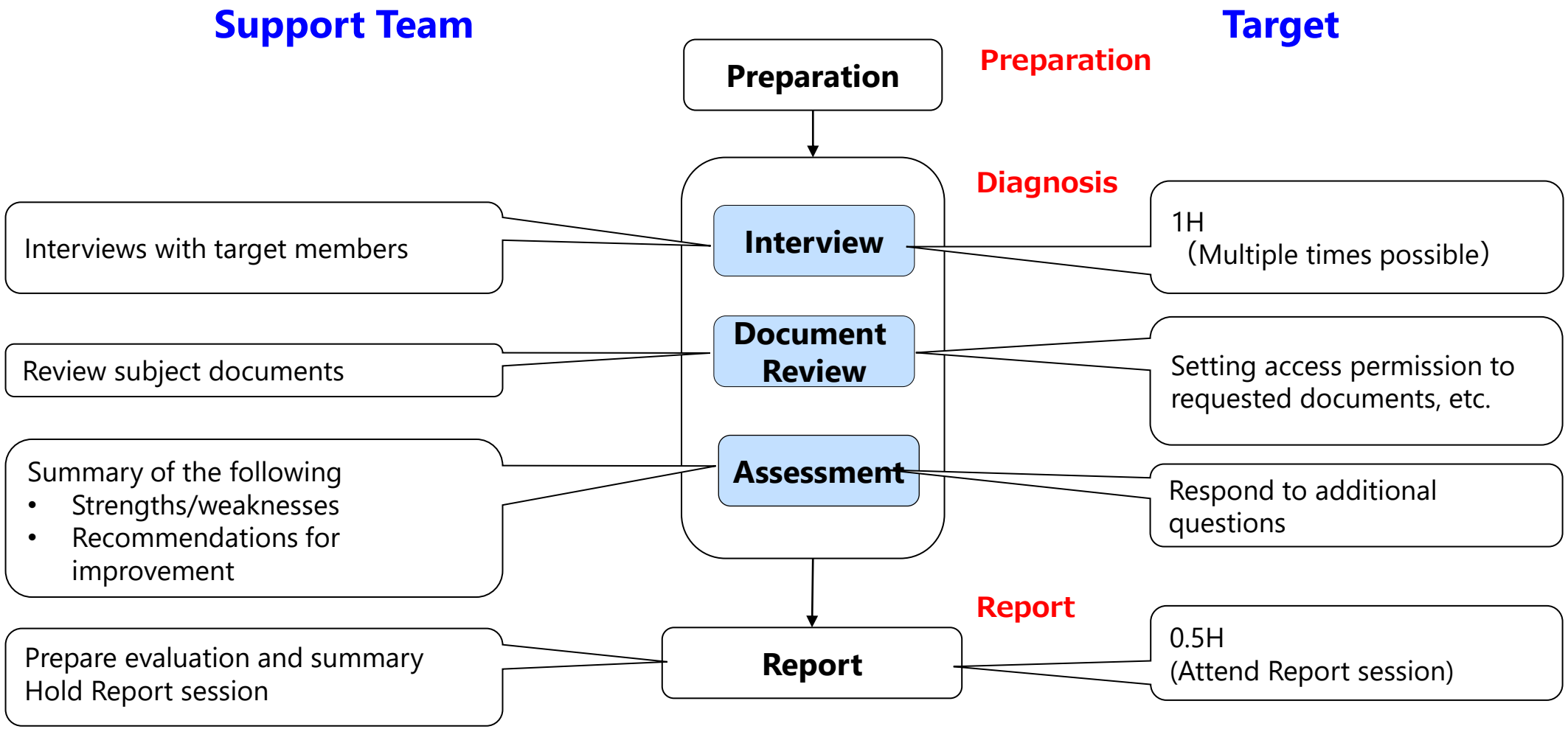
Objectively evaluate the current status of OSS management

- Utilize ISO/IEC 5230 (OpenChain specification) to identify issues
- Identify organizational strengths and opportunities for improvement



Example of Improvement Diagnosis

Interview, Review, Assessment, Report



02

Case Study

Masaya Tarui

Open Source Program Manager
at Digital Innovation Technology Center (DITC)

Work Experience

2001~ R&D HW/SW Test, Co-design, CAD
2018~ R&D DNN-acc, Cloud Computing
2019~ DITC HABANEROTS* (BaaS)

Open Source

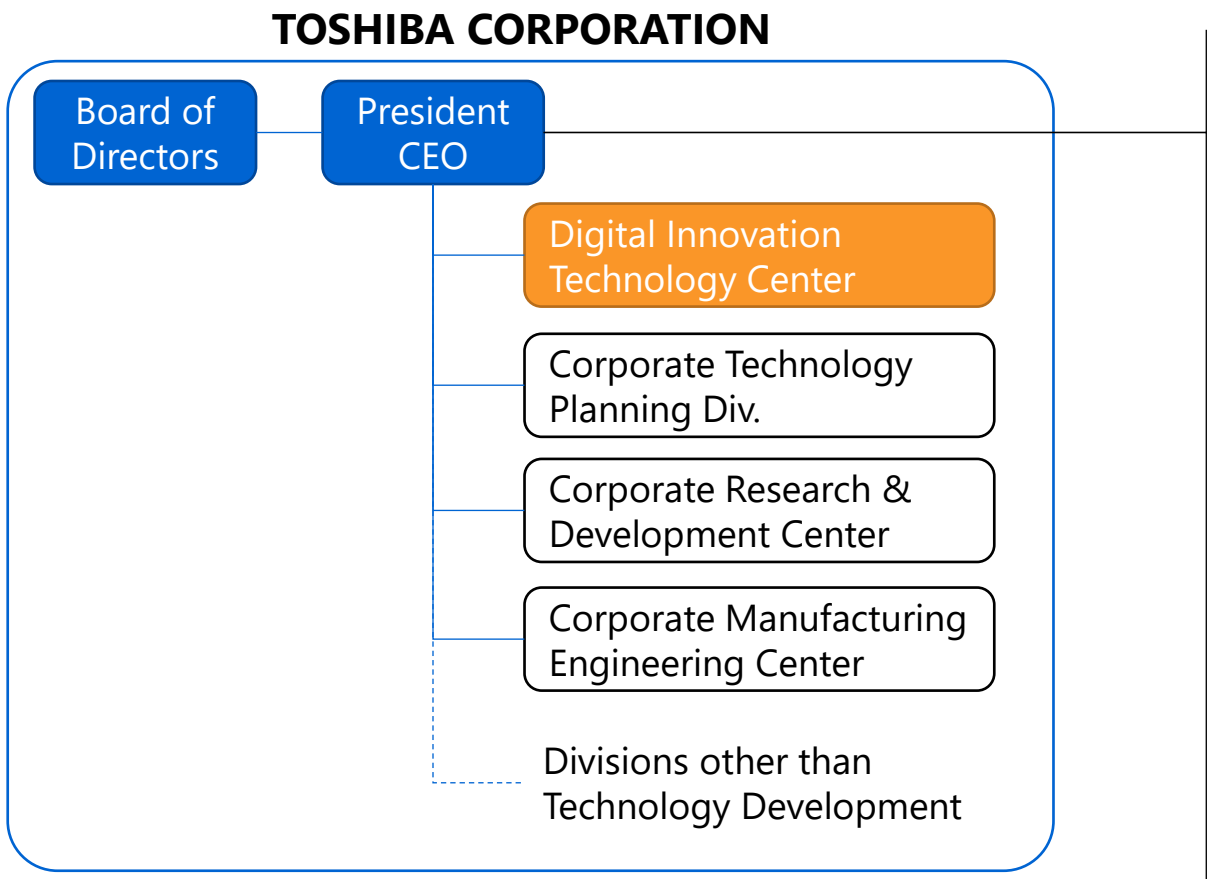
2006~ Contributing to Ruby
2010~ Core Committer of Ruby
Focusing performance improvement, timing bugs, etc.

*HABANEROTS: Toshiba Industrial IoT Platform Service
A cloud-native microservices environment consists of OSS such as Kubernetes and more.
Also see the following document:
https://www.global.toshiba/content/dam/toshiba/ww/technology/corporate/review/2020/high2020/2002.pdf

Digital Innovation Technology Center (DITC)

Mission

Develop & Deploy B2B As-a-Service family



Energy Systems & Solutions
- Toshiba Energy System & Solutions Corporation
- Toshiba Plant Systems & Service Corporation

Infrastructure Systems & Solutions
- Toshiba Infrastructure Systems & Solution Corporation

Building Solutions
- Toshiba Elevator and Building Systems Corporation
- Toshiba Lighting & Technology Corporation
- Toshiba Carrier Corporation

Retail & Printing Solutions
- Toshiba Tec Corporation

Electronic Device & Storage Solutions
- Toshiba Electronic Devices & Storage Corporation

Digital Solutions
- Toshiba Digital Solution Corporation

Start of efforts (2021/4/E～)

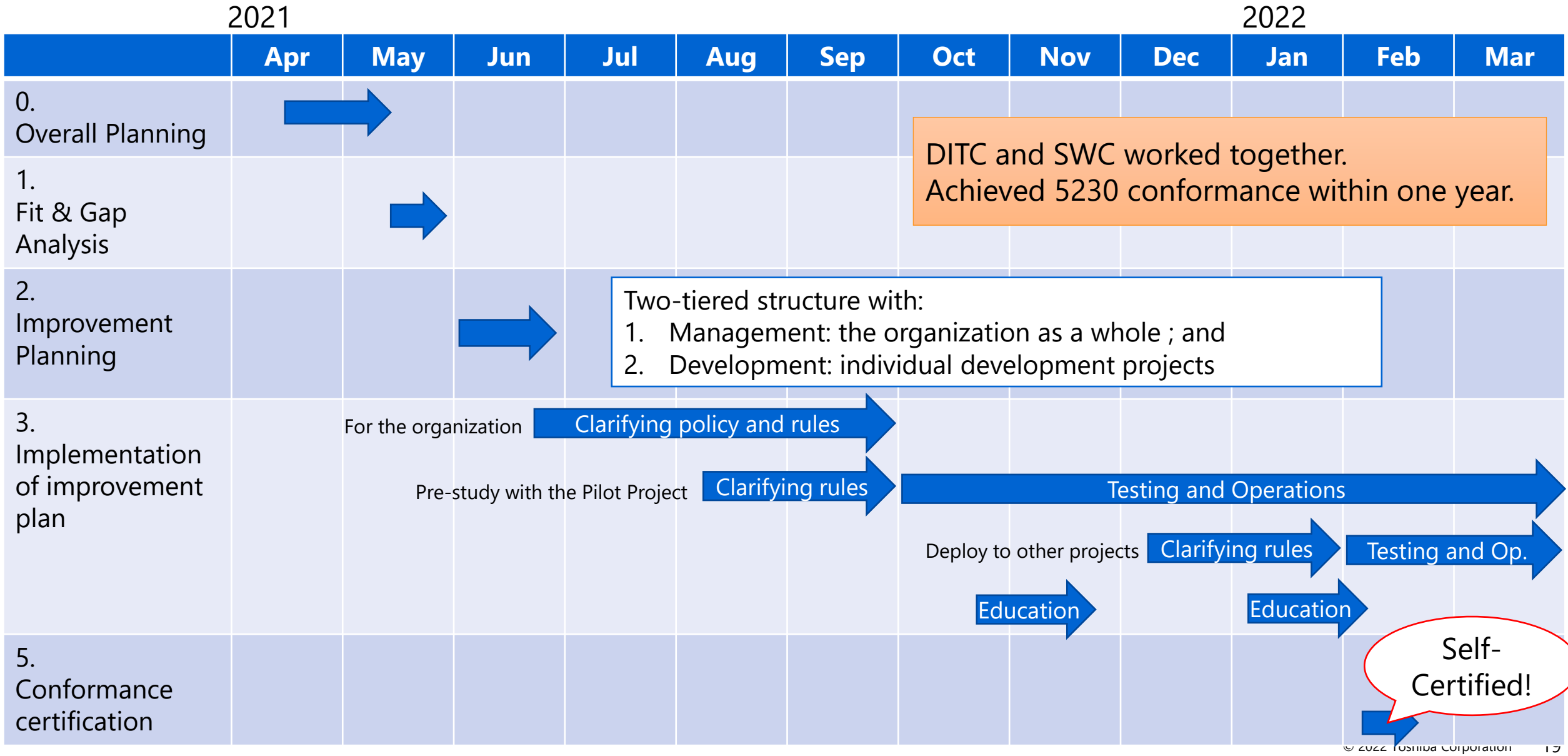
Initiative Team
Experienced Open Source Developer and Manager

Improvement Support Team
SPI expert and OSS expert from SWC

OpenChain's vision matches DITC's policy. Therefore, the achievement of conformance was considered to strengthen the organization.

- **OpenChain's Vision**
  1. Developing Open Source Ecosystem with Compliance
- **DITC's Policy (DITC will:)**
  1. Develop and improve Toshiba's digital infrastructure and presence
  2. Contribute to OSS
  3. Be a model case for Toshiba Group

Journey to 5230 Compliance Certification



Fit & Gap Analysis

License compliance was almost implemented.
But, Gap exists with 5230 specifications.

Subjects to improvement

1. Establishment of organizational structure
2. Defining Competence
3. Documentation
4. Education

Improving (1/5)

Two-tiered structure with organization and projects

Subjects to improvement

1. **Establishment of organizational structure**
2. **Defining Competence**
3. Documentation
4. Education

- **Competence**

Manager, Program Owner, Product Lead, Contact, IP/Legal, Procurement, Quality Control, Open Source Management Board

- **Scope and management**

Organization

- Fundamental Policy
- Education
- Evidence management
- Requirements for each project

Project

- Ensure Resource
- Open Source License Policy
- Quality Control Policy

Balancing project **discretion** and **flexibility**

Improving (2/5)

Documentation: Policy and Process

Subjects to improvement

1. Establishment of organizational structure
2. Defining Competence
3. **Documentation**
4. Education

Organization: Policy

- Fundamental Policy
- Scope
- Structure
- Quality Control
- Security
- Education
- Resource
- Contact
- SCA and SBOM

and more…

Project: Policy in Details (ex.)

- Fundamental Policy
- Scope
- Structure
- Quality Control
- Security
- Education
- Resource
- Contact
- SCA and SBOM
- and more…

Documentation: Policy and Process

Subjects to improvement

1. Establishment of organizational structure
2. Defining Competence
3. **Documentation**
4. Education

- **SBOM**

  Some items are changed as mandatory
  (ex. Source of acquisition. such as URLs)

- **Evidence Management**

  Change Management entity and workflow
  Before: Project driven
  After: Centralized within the organization

Improving (4/5)

Visibility and Transparency

Subjects to improvement

1. Establishment of organizational structure
2. Defining Competence
3. Documentation
4. **Education**

- **Sessions**
  - For all members (including Management)
  - Commentary and Q&A on Policy, Process and Rule

- **Documentations**
  - Available at any time (internally)

Improving (5/5)

All members take E-learning

Subjects to improvement

1. Establishment of organizational structure
2. Defining Competence
3. Documentation
4. **Education**

- **E-learning**
  - Two levels of content (produced by SWC)
  - Capable of managing learning history

Level	Topics	Targets
Pre-Basic	Open Source Software, Open Source License, Overview of precautions in using OSS, etc.	Anyone involved in product development
Basic	Key points, Workflow, and Cautions of the OSS management process	Developer, Quality Control, IP/Legal

Summary of the self-certification

Requirements	Headings	After
1. Program foundation	1.1 Policy	○
	1.2 Competence	○
	1.3 Awareness	○
	1.4 Program scope	○
	1.5 License obligations	○
2. Relevant tasks defined and supported	2.1 Access	○
	2.2 Effectively resourced	○
3. Open source content review and approval	3.1 Bill of Materials	○
	3.2 License compliance	○
4. Compliance artifact creation and delivery	4.1 Compliance artifacts	○
5. Understand open Source community engagement	5.1 Contributions	○
6. Adherence to the Specification Requirements	6.1 Conformance	○
	6.2 Duration	○

Summary of the self-certification (cont'd)

Strength

- Defining policies and management processes/procedures
  Members of the organization are aware of them
  - (§1.1 Policy, §1.3 Recognition, §3.1 Bill of Materials)
- Assigning person in charge of Open Source Program, Defining competencies for each role, and Providing Education
  - (§1.2 Competencies)
- Implementing initiatives of operation and management for each product
  - (§1.4 Scope of program, §1.5 License obligations, §2.2 Adequate resource allocation, §3.1 Bill of materials, §3.2 License compliance)
- Compliance with ISO/IEC5230
  - (§6 (ISO/IEC5230) Compliance with specification requirements)

Key Points for Success

- Experienced Open Source Developer’s Leadership
- Management’s Endorsement
- Two-tiered structure with organization and projects
- Leverage Existing framework
- Well-communication

Several issues for further improvement

- Trade-off between workload and discretion
- Need for more light-weight management processes with keeping compliance (e.g. contributions)

DITC’s Open Source Policy (summary)

DITC will develop and improve **Toshiba's digital infrastructure and presence** in perspective over the medium to long term. DITC will also produce **deliverables of OSS and ISS, and contribute to OSS**, in cooperation with other organizations.

This activity shall strive to be **a model for other organizations**.

We will continue to create and share knowledge and values as a member of the open source community.

Thank you!

TOSHIBA