SECCOM CII Badging

What Does it Mean to Get Gold in CII Badging?
(and Silver and Passing)

SECCOM

Tony Hansen

2019/9/27

What is CII Badging About?

"The Linux Foundation (LF) Core Infrastructure Initiative (CII) Best Practices badge is a way for Free/Libre and Open Source Software (FLOSS) projects to show that they follow best practices."

bestpractices.coreinfrastructure.org

". . . following best practices can help improve the results of projects. For example, some practices enable multi-person review before release, which can both help find otherwise hard-to-find technical vulnerabilities and help build trust and a desire for repeated interaction among developers from different organizations.''

github.com/coreinfrastructure/best-practices-badge/blob/master/doc/criteria.md

"Compare the cost of defense to the cost of failure"
"Take the software equivalent of basic hygiene steps and combine approaches in a way that make a system harder to successfully attack"
"Failing to implement basic measures for protection, detection and recovery in systems where it matters is just a form of negligence"
"It is an easy way for an open source project to self-improve." – Dr. David A. Wheeler

How to Develop Secure Applications: The BadgeApp Example

www.youtube.com/watch?v=5a5D4d6hcEY

Creator of the BadgeApp application

Author: Secure Programming: HOWTO dwheeler.com/secure-programs

Some Badge Earniers







Why are we doing this?

Bottom line: We are using CII Badging to get ONAP projects to verify and/or improve the security and quality of their code and the project.

Getting the silver star or gold star from the CII badge is truly secondary.

Progressively Strict

- The three levels are Passing, Silver and Gold
- The questions use SHOULD and MUST to differentiate between Optional (at this level) and Requirements
- Questions will progress across levels:
- An item introduced in Passing as a SHOULD will become a MUST in Silver
- An item introduced in Silver as a SHOULD will become a MUST in Gold

Answering a SHOULD question as YES counts at ALL LEVELS.

The CII Sections

Passing	Silver	Gold
Basics	Basics	Basics
Change Control	Change Control	Change Control
Reporting	Reporting	
Quality	Quality	Quality
Security	Security	Security
Analysis	Analysis	Analysis

How is ONAP Doing on Badging Levels?

Passing:

- 30 / 34 are 100% Passing
- Remaining 4 are >85% Passing

Silver:

- 2 are 100% Silver – Wow
- 25 are >75% Silver – Super
- 4 are 30% to 45%
- 7 are < 30%

Gold:

- 5 > 40% – Cool
- 8 are 20% to 40%
- 25 are < 20%

Multiple Categories of Concern

I've categorized the different questions using these categories for separate domains of questions:

- The quality of the application itself
- The quality of the project overview
- The quality of the infrastructure used to build and support the application
- The people building the application
- FLOSS encouragement

	Passing	Silver	Gold
Application Quality	26	24	9
Project Quality	22	26	8
Infrastructure Quality	10	2	4
People	4	3	2
FLOSS Encouragement	4		
Totals	66	55	23

The Silver Criteria

Project Quality

code of conduct
coding standards
coding standards enforced
contribution requirements
developer cert. of origin
documentation achievements
documentation architecture
documentation current
documentation quick start
documentation roadmap
external dependencies
governance
installation common
installation development quick
installation standard variables
maintenance or update
report tracker
signed releases
test policy mandated
tests documented added
updateable reused comp's
version tags signed
vulnerability report credit
vulnerability resp process

Application Quality

accessibility best practices
assurance case
automated int. testing
build non recursive
build preserve debug
build repeatable
build standard variables
crypto algorithm agility
crypto cert. verification
crypto credential agility
crypto tls12
crypto used network
crypto verification private
crypto weaknesses
dependency monitoring
dynamic analysis unsafe
hardening
implement secure design
input validation
interfaces current
internationalization
regression tests added50
static analysis common vulnerabilities
test statement cvrg 80
warnings strict

People

access continuity
bus factor
roles responsibilities

Infrastructure Quality

documentation security
sites password security

The Gold Criteria

Application quality

- *Two person reviews*
- *Crypto TLS12*
- *Crypto Used Network*
- **Application Hardening**
- **Dynamic Analysis Tool**
- **Security Reviews**
- **80% test branch coverage**
- **Test suite invocation standardized**
- **90% statement test coverage**

Project Quality

- *License per file*
- *Copyright per file*
- *Continuous Integration*

- **Reproducible Build**
- **Code Review Standards**
- **>=2 Unassociated Contributors per project**

People

- **Bus Factor**
- **Small Tasks for new / casual contributors**

Infrastructure Quality

- *Distributed Repo Tools*
- **Hardened Site**
- **2FA for contributors**

Resources

CII Site

https://bestpractices.coreinfrastructure.org

EXTENSIVE DETAILS ON THE CII QUESTIONS

https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/criteria.md
https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/other.md

Why these questions?
https://github.com/coreinfrastructure/best-practices-badge/blob/master/doc/background.md

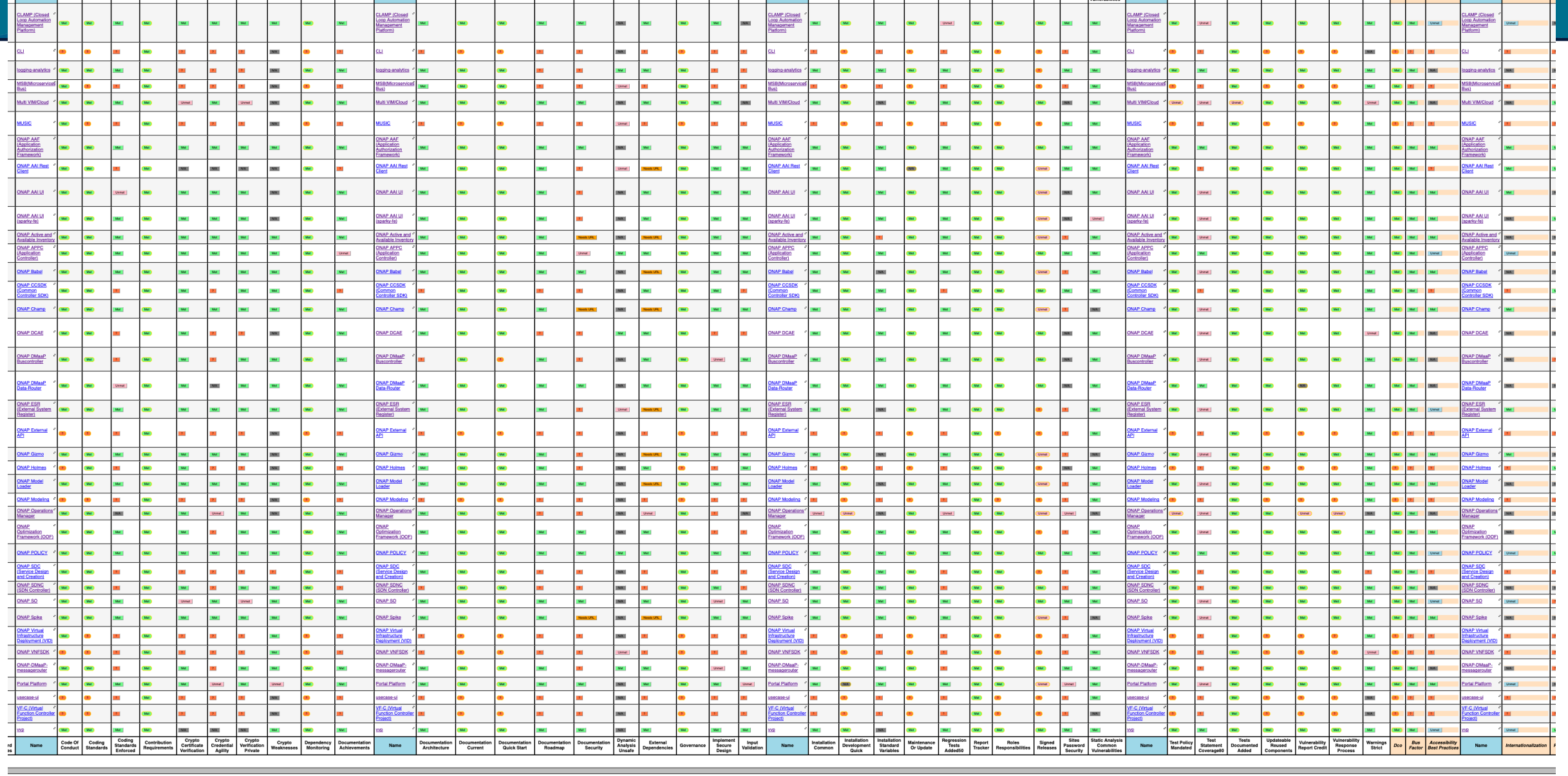
ONAP Resources, including answers to many “questions with ONAP-wide answers”:
https://wiki.onap.org/display/DW/CII+Badging+Program

CII ONAP Portal
http://tlhansen.us/onap/cii.html

Code of conduct

Crypto certificate verification

Crypto used network



Name	Code Of Conduct	Coding Standards	Coding Standards Enforced	Contribution Requirements	Crypto Certificate Verification	Crypto Credential Agility	Crypto Verification Private	Crypto Weaknesses	Dependency Monitoring	Documentation Achievements	Name	Documentation Architecture	Documentation Current	Documentation Quick Start	Documentation Roadmap	Documentation Security	Dynamic Analysis Unsafe	External Dependencies	Governance	Implement Secure Design	Input Validation	Name	Installation Common	Installation Development Quick	Installation Standard Variables	Maintenance Or Update	Regression Tests Added50	Report Tracker	Roles Responsibilities	Signed Releases	Sites Password Security	Static Analysis Common Vulnerabilities	Name	Test Policy Mandated	Test Statement Coverage80	Tests Documented Added	Updateable Reused Components	Vulnerability Report Credit	Vulnerability Response Process	Warnings Strict	Dco	Bus Factor	Accessibility Best Practices	Name	Internationalization	P
CLAMP (Closed Loop Automation Management Platform)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	CLAMP (Closed Loop Automation Management Platform)	Met	Met	Met	Met	Met	N/A	Met	Met	Met	N/A	CLAMP (Closed Loop Automation Management Platform)	Met	Met	Met	Met	Unmet	Met	Met	Met	Met	CLAMP (Closed Loop Automation Management Platform)	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Unmet	CLAMP (Closed Loop Automation Management Platform)	Unmet	
CLI	?	?	?	Met	?	?	?	N/A	?	?	CLI	?	?	?	?	?	N/A	?	?	?	?	CLI	?	?	?	?	?	Met	?	?	?	Met	CLI	?	?	Met	?	?	?	N/A	?	?	?	CLI	?	
logging-analytics	Met	Met	Met	Met	?	?	?	N/A	Met	Met	logging-analytics	Met	Met	Met	?	?	Met	Met	Met	?	?	logging-analytics	Met	Met	Met	Met	Met	Met	Met	?	Met	Met	logging-analytics	Met	Met	Met	Met	Met	Met	Met	Met	Met	N/A	logging-analytics	N/A	
MSB(Microservice Bus)	Met	?	?	Met	?	?	?	N/A	?	?	MSB(Microservice Bus)	Met	Met	Met	?	Unmet	?	Met	?	?	?	MSB(Microservice Bus)	?	?	?	?	?	Met	Met	?	?	Met	MSB(Microservice Bus)	?	?	Met	?	?	?	Met	Met	?	?	MSB(Microservice Bus)	?	
Multi VIM/Cloud	Met	Met	Met	Met	Unmet	Met	Unmet	N/A	Met	Met	Multi VIM/Cloud	Met	Met	Met	Met	Met	N/A	Met	Met	Met	N/A	Multi VIM/Cloud	Met	Met	N/A	Met	Met	Met	Met	N/A	Met	Unmet	Multi VIM/Cloud	Unmet	Unmet	Unmet	Met	Met	Met	Unmet	Met	Met	N/A	Multi VIM/Cloud	N/A	
MUSIC	?	?	?	Met	?	?	?	N/A	?	?	MUSIC	?	?	?	?	?	Unmet	?	?	?	?	MUSIC	?	?	?	?	?	Met	?	?	Met	?	MUSIC	?	?	Met	?	?	?	Met	?	?	?	MUSIC	?	
ONAP AAF (Application Authorization Framework)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP AAF (Application Authorization Framework)	Met	Met	Met	Met	Met	N/A	Met	Met	Met	Met	ONAP AAF (Application Authorization Framework)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP AAF (Application Authorization Framework)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP AAF (Application Authorization Framework)	Met	
ONAP AAI Rest Client	Met	Met	?	Met	N/A	N/A	N/A	N/A	Met	?	ONAP AAI Rest Client	Met	Met	Met	Met	?	Unmet	Needs URL	Met	Met	Met	ONAP AAI Rest Client	Met	Met	Met	Met	N/A	Met	Met	Unmet	Met	Met	ONAP AAI Rest Client	Met	?	Met	Met	Met	Met	Met	Met	Met	?	ONAP AAI Rest Client	Met	
ONAP AAI UI	Met	Met	Unmet	Met	Met	Met	Met	N/A	Met	Met	ONAP AAI UI	Met	Met	Met	Met	?	N/A	Met	Met	Met	Met	ONAP AAI UI	Met	Met	Met	Met	Met	Met	Met	Unmet	N/A	Met	ONAP AAI UI	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Met	ONAP AAI UI	Met	
ONAP AAI UI (sparky-fe)	Met	Met	Met	Met	Met	Met	Met	N/A	Met	Met	ONAP AAI UI (sparky-fe)	Met	Met	Met	Met	?	N/A	Met	Met	Met	Met	ONAP AAI UI (sparky-fe)	Met	Met	Met	Met	Met	Met	Met	Unmet	N/A	Unmet	ONAP AAI UI (sparky-fe)	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP AAI UI (sparky-fe)	N/A	
ONAP Active and Available Inventory	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Active and Available Inventory	Met	Met	Met	Met	Needs URL	N/A	Needs URL	Met	Met	Met	ONAP Active and Available Inventory	Met	Met	Met	?	Met	Met	Met	Unmet	?	Met	ONAP Active and Available Inventory	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP Active and Available Inventory	N/A	
ONAP APPC (Application Controller)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Unmet	ONAP APPC (Application Controller)	Met	Met	Met	Met	Unmet	Met	Met	Met	Met	Met	ONAP APPC (Application Controller)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP APPC (Application Controller)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Unmet	ONAP APPC (Application Controller)	Unmet	
ONAP Babel	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Babel	Met	Met	Met	Met	Met	N/A	Needs URL	Met	Met	Met	ONAP Babel	Met	Met	Met	N/A	Met	Met	Met	Unmet	?	Met	ONAP Babel	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP Babel	N/A	
ONAP CCSDK (Common Controller SDK)	Met	Met	?	Met	Met	?	Met	Met	Met	?	ONAP CCSDK (Common Controller SDK)	?	Met	Met	?	?	N/A	Met	Met	?	?	ONAP CCSDK (Common Controller SDK)	Met	Met	Met	Met	?	Met	Met	Met	Met	Met	ONAP CCSDK (Common Controller SDK)	Met	?	Met	Met	Met	Met	Met	Met	?	?	ONAP CCSDK (Common Controller SDK)	?	
ONAP Champ	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Champ	Met	Met	Met	Met	Needs URL	N/A	Needs URL	Met	Met	Met	ONAP Champ	Met	Met	Met	Met	Met	Met	Met	Unmet	?	N/A	ONAP Champ	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP Champ	Met	
ONAP DCAE	Met	Met	?	Met	Met	?	?	N/A	Met	Met	ONAP DCAE	Met	Met	Met	?	?	Met	Met	Met	?	?	ONAP DCAE	Met	Met	Met	Met	Met	Met	Met	Met	N/A	Met	ONAP DCAE	Met	Unmet	Met	Met	Met	Met	Unmet	Met	Met	N/A	ONAP DCAE	N/A	
ONAP DMaaP Buscontroller	Met	Met	?	Met	Met	?	Met	Met	Met	Met	ONAP DMaaP Buscontroller	?	Met	?	Met	?	N/A	Met	Met	Unmet	Met	ONAP DMaaP Buscontroller	Met	Met	Met	Met	Met	Met	Met	Met	N/A	Met	ONAP DMaaP Buscontroller	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP DMaaP Buscontroller	N/A	
ONAP DMaaP Data-Router	Met	Met	Unmet	Met	Met	N/A	Met	Met	Met	Met	ONAP DMaaP Data-Router	Met	Met	Met	Met	Met	N/A	Met	Met	Met	Met	ONAP DMaaP Data-Router	Met	Met	Met	Met	Met	Met	Met	Met	N/A	Met	ONAP DMaaP Data-Router	Met	Met	Met	Met	N/A	Met	Met	Met	Met	N/A	ONAP DMaaP Data-Router	N/A	
ONAP ESR (External System Register)	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP ESR (External System Register)	Met	Met	Met	Met	?	Unmet	Needs URL	Met	Met	Met	ONAP ESR (External System Register)	Met	Met	N/A	Met	Met	?	?	Met	Met	Met	ONAP ESR (External System Register)	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Unmet	ONAP ESR (External System Register)	Met	
ONAP External API	?	?	?	Met	?	?	?	N/A	?	?	ONAP External API	?	?	?	?	?	N/A	?	?	?	?	ONAP External API	?	?	?	?	?	Met	?	?	?	Met	ONAP External API	?	?	Met	?	?	?	Met	?	?	?	ONAP External API	?	
ONAP Gizmo	Met	Met	Met	Met	Met	Met	Met	N/A	Met	Met	ONAP Gizmo	Met	Met	Met	Met	?	N/A	Needs URL	Met	Met	Met	ONAP Gizmo	Met	Met	N/A	Met	Met	Met	Met	Unmet	?	N/A	ONAP Gizmo	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP Gizmo	Met	
ONAP Holmes	?	Met	?	Met	Met	?	?	N/A	Met	?	ONAP Holmes	Met	Met	Met	Met	?	N/A	Met	?	?	Met	ONAP Holmes	?	?	?	?	?	Met	Met	?	N/A	Met	ONAP Holmes	?	?	Met	?	?	?	Met	?	?	?	ONAP Holmes	?	
ONAP Model Loader	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Model Loader	Met	Met	Met	Met	Met	N/A	Needs URL	Met	Met	Met	ONAP Model Loader	Met	Met	N/A	Met	Met	Met	Met	Unmet	?	Met	ONAP Model Loader	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Model Loader	N/A	
ONAP Modeling	?	?	?	Met	?	?	?	N/A	?	?	ONAP Modeling	?	?	?	?	?	N/A	?	?	?	?	ONAP Modeling	?	?	?	?	?	Met	?	?	?	Met	ONAP Modeling	?	?	Met	?	?	?	Met	?	?	?	ONAP Modeling	?	
ONAP Operations Manager	Met	Met	N/A	Met	Met	Unmet	Met	N/A	Met	Met	ONAP Operations Manager	Met	Met	Met	?	?	N/A	Unmet	Met	?	N/A	ONAP Operations Manager	Unmet	Unmet	N/A	Met	Unmet	N/A	Met	Met	N/A	N/A	ONAP Operations Manager	Unmet	Unmet	Met	Met	Unmet	Unmet	N/A	Met	Met	N/A	ONAP Operations Manager	N/A	
ONAP Optimization Framework (OOF)	Met	Met	Met	Met	Met	?	Met	Met	Met	Met	ONAP Optimization Framework (OOF)	Met	Met	Met	Met	Met	N/A	Met	Met	?	?	ONAP Optimization Framework (OOF)	Met	Met	Met	Met	Met	Met	Met	?	?	Met	ONAP Optimization Framework (OOF)	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Optimization Framework (OOF)	N/A	
ONAP POLICY	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP POLICY	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP POLICY	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP POLICY	Met	Met	Met	Met	Met	Met	Met	Met	Met	Unmet	ONAP POLICY	Unmet	
ONAP SDC (Service Design and Creation)	Met	Met	?	Met	?	?	?	?	Met	?	ONAP SDC (Service Design and Creation)	Met	Met	Met	?	?	N/A	?	Met	?	?	ONAP SDC (Service Design and Creation)	Met	Met	Met	Met	?	Met	Met	?	Met	Met	ONAP SDC (Service Design and Creation)	Met	?	Met	Met	Met	Met	?	Met	Met	?	ONAP SDC (Service Design and Creation)	?	
ONAP SDNC (SDN Controller)	Met	Met	?	Met	Met	?	Met	Met	Met	?	ONAP SDNC (SDN Controller)	?	Met	Met	?	?	N/A	?	Met	Met	?	ONAP SDNC (SDN Controller)	Met	Met	Met	Met	?	Met	Met	?	Met	Met	ONAP SDNC (SDN Controller)	Met	?	Met	Met	Met	Met	Met	Met	Met	N/A	ONAP SDNC (SDN Controller)	N/A	
ONAP SO	Met	Met	Met	Met	Unmet	Met	Unmet	Met	Met	Met	ONAP SO	Met	Met	Met	Met	Met	N/A	Met	Met	Unmet	Met	ONAP SO	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP SO	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Unmet	ONAP SO	Unmet	
ONAP Spike	Met	Met	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Spike	Met	Met	Met	Met	Needs URL	N/A	Needs URL	Met	Met	Met	ONAP Spike	Met	Met	Met	Met	Met	Met	Met	Unmet	?	N/A	ONAP Spike	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Met	ONAP Spike	N/A	
ONAP Virtual Infrastructure Deployment (VID)	Met	?	?	Met	?	?	?	Met	?	?	ONAP Virtual Infrastructure Deployment (VID)	?	?	?	?	?	N/A	?	?	?	?	ONAP Virtual Infrastructure Deployment (VID)	?	?	?	?	?	Met	?	?	?	Met	ONAP Virtual Infrastructure Deployment (VID)	?	?	Met	?	?	?	Met	?	?	Unmet	ONAP Virtual Infrastructure Deployment (VID)	?	
ONAP VNFSDK	?	?	?	Met	?	?	?	Met	?	?	ONAP VNFSDK	?	?	?	?	Unmet	?	?	?	?	?	ONAP VNFSDK	?	?	?	?	?	Met	?	?	?	Met	ONAP VNFSDK	?	?	Met	?	?	?	Met	?	?	Unmet	ONAP VNFSDK	?	
ONAP-DMaaP-messagerouter	Met	Met	?	Met	Met	?	Met	Met	Met	Met	ONAP-DMaaP-messagerouter	Met	Met	Met	Met	?	Met	Met	Met	Unmet	Met	ONAP-DMaaP-messagerouter	Met	Met	Met	Met	?	Met	Met	Met	Met	Met	ONAP-DMaaP-messagerouter	Met	?	Met	Met	Met	Met	N/A	Met	Met	?	ONAP-DMaaP-messagerouter	N/A	
Portal Platform	Met	Met	Met	Met	Met	Unmet	Met	Unmet	Met	Met	Portal Platform	Met	Met	Met	Met	Met	N/A	Met	Met	Unmet	Met	Portal Platform	Met	N/A	Met	Met	Met	Met	Met	Unmet	Unmet	Met	Portal Platform	Met	Unmet	Met	Met	Met	Met	Met	Met	Met	Met	Portal Platform	Unmet	
usecase-ui	?	?	?	Met	?	?	?	N/A	?	?	usecase-ui	?	?	?	?	?	N/A	?	?	?	?	usecase-ui	?	?	?	?	?	Met	?	?	?	Met	usecase-ui	?	?	Met	?	?	?	N/A	?	?	?	usecase-ui	?	
VF-C (Virtual Function Controller Project)	?	?	?	Met	?	?	?	N/A	?	?	VF-C (Virtual Function Controller Project)	?	?	?	?	?	N/A	?	?	?	?	VF-C (Virtual Function Controller Project)	?	?	?	?	?	Met	?	?	N/A	Met	VF-C (Virtual Function Controller Project)	?	?	Met	?	?	?	N/A	?	?	?	VF-C (Virtual Function Controller Project)	?	
vvp	Met	Met	Met	Met	N/A	N/A	N/A	Met	Met	Met	vvp	Met	Met	Met	Met	Met	N/A	Met	Met	Met	N/A	vvp	Met	Met	N/A	Met	Met	Met	Met	Met	Met	Met	vvp	Met	Met	Met	Met	Met	Met	Met	Met	Met	Unmet	vvp	Unmet	
Name	Code Of Conduct	Coding Standards	Coding Standards Enforced	Contribution Requirements	Crypto Certificate Verification	Crypto Credential Agility	Crypto Verification Private	Crypto Weaknesses	Dependency Monitoring	Documentation Achievements	Name	Documentation Architecture	Documentation Current	Documentation Quick Start	Documentation Roadmap	Documentation Security	Dynamic Analysis Unsafe	External Dependencies	Governance	Implement Secure Design	Input Validation	Name	Installation Common	Installation Development Quick	Installation Standard Variables	Maintenance Or Update	Regression Tests Added50	Report Tracker	Roles Responsibilities	Signed Releases	Sites Password Security	Static Analysis Common Vulnerabilities	Name	Test Policy Mandated	Test Statement Coverage80	Tests Documented Added	Updateable Reused Components	Vulnerability Report Credit	Vulnerability Response Process	Warnings Strict	Dco	Bus Factor	Accessibility Best Practices	Name	Internationalization	P

Thank you

That’s all

Q & A