

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 <u>Linux Foundation (LF)</u> <u>Core Infrastructure Initiative (CII)</u> 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 build 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 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



d) Name	Code Of	Coding Standards	Coding Standards	Contribution Requirements	Crypto Certificate Verification	Crypto Credential Agility	Crypto Verification Private	Crypto Weaknesser	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 Inst	allation Installation opment Standard	Maintenance Or Update	Regression Tests Added50	Report Tracker	Roles Si Responsibilities Rel	gned Passy eases Secu	s Static Analysis Common Vulnerabilities	Name F	Fest Toolicy State	est Test ement Docume rage80 Adde	s Updateable nted Reused d Component	Vulnerability Report Credit	Vulnerability Response Process	Warnings Strict	Dco Bus Factor	Accessibility Best Practices	Name	Internationalization
•	, Johnson	Standards	Enforced	quarametris	Verification	Agility	Private		mormoring	- Constanting			Content	QUICK SIGHT	повинар	Security	Unsafe	- periodicies		Design	- Lineauon			ulck Variable	or opulate	Added50	acner		Secu	Vulnerabilities		ndated Cove	rage80 Adde	d Component	Credit	Process	Suici	racior	Practices	CLAMP (Closed	
CLAMP (Closed Loop Automation Management Platform)	Mel	w	Med	(MIC)	Met	Met	Met	Met	(Mar)	Met	CLAMP (Closed Loop Automation Management Platform)	[Mel]	(MA)	(MA)	Met	[Me]	INAL	Not .	(MI)	Met	INK	CLAMP (Closed Loop Automation Management Platform)	[Mel] (Mel)	Met	(Mil)	Unnet	Mat	(Mil)	ME	Met	CLAMP (Closed ** Loop Automation Management Platform)	Unmail		(Mel)	(Mel)	(MI)	Med	Mac Mac	Usnet	CLAMP (Closed Loop Automation Management Platform)	Unnet
CLI		•	-	Met	-	101		INA			CLI	-			-	2	NA.	191	-	2	191	cu r		7		-	Wat		-	Mut	aı ·	-	Mac				INA	0	7	a .	
logging-analytics	· (Net)	Wet	Bloc	Met	120	181	191	[NA]	Mat	Met	logging-analytics	· we	Met	(Mat)		2	Vit	Met	Met	121	121	logging-analytics "	Mot	Met	Met	Met	Wat	(Max)	Mot	Nut	logging-analytics *	Mat	Mar	Met	Met	Met	Bidge	Mac Mac	[NAT	logging-analytics *]NX
MSB(Microserviou Bus)	· ·		181	(Met)	100	INI	191	INAI		21	MSB(Microservice Bus)	S MARI	(Mil)	(Ma)			Urmet	120	(MI)	100	<u> </u>	MSB(Microservices Bus)	M 00	121	35	101	Wet	(M)	131	Met	MSB(Microservices Bus)		Mat	(3)	60	20	TANK (Mat 12	12	MSB(Microservices Bus)	M
Multi VIM/Cloud	· Man	(Max)	Mot	(Mat)	Unnet	Met	Unnet	INA	(Mac)	Mat	Multi VIM/Cloud	- uu	Met	(Max)	Wet	Met	INKI	Wet	Mee	Met	INK	Multi VIM/Cloud *	Met Met	INA	(Met)	blet	(Mat)	(Max) (Max	INKI	Mat	Multi VIM/Cloud ** (III	met United	(Unmat)	Man	(Met)	Met	Unwet	Mac Mac	[RAT	Multi VIM/Cloud	INK
MUSIC ONAP AAF	1	•		(Met)	-	101	,	INA	•	2	MUSIC ONAP AAF	1		90		7	Urmet	191		121		MUSIC *		17			(Met.)	• •	Met	Met	MUSIC	-	(Mat)	-		***	Med	2) [2]	17	MUSIC *	
ONAP AAF (Application Authorization Framework)	Met	Wat	Mot	(MIC)	Met	Met	Met	Met	(Mar)	Met	ONAP AAF (Application Authorization Framework)	16dd	(Md)	(Ma)	Met	Met	INK	Met	(Met)	Met	Met	ONAP AAF (Application Authorization Framework)	Met	Met	(Met)	Met	Wet	(Max)	i Mari	Met	ONAP AAF (Application Authorization Framework)	D Mari	(Mar)	Mel	(Met)	(Met)	Mati	Mat Mat	Mar	ONAP AAF (Application Authorization Framework)	Met
ONAP AAI Best Client	· ·	(Me)	-	(Mel)	NAT	INA	N/A	[NA]	(Me)	-	ONAP AAI Rest Client		(Mil)	(Ma)	Met		Urmet	Noon U.	(MI)	Me	Met	ONAP AAI Rest Client	Me! Me	Met	(NAX)	Met	Wat	(Mil)	mat Mat	Met	ONAP AAI Rest Client		Met	Mel	(Met)	Mil	[Mari]	MH MH	7	ONAP AAI Rost Client	Met
ONAP AAI UI	· Mail	w	Unnet	(Met)	Met	Met	Met	INAI	(Mar)	Mat	ONAP AAI UI	· wei	(MI)	w	Met	IMI	NA	[Mr]	(MI)	Met	Met	ONAP AAI UI	Mel	Met	(Mil)	MART	(Mat.)	(Us	nd) NAI	Met	ONAP AAI UI	Unmal	(Mar)	Mel	(Met)	Mil	Mil	ми	Mil	ONAP AAI UI	Met
ONAP AAI UI (sparky-fe)	, Mac	We	Mot	Mac	Met	Met	Met	[NA]	(Mac)	Net	ONAP AAI UI (sparky-fe)	· 1861	MAL	(Max	Met	1001	NX	Met	Mat	Met	Net	ONAP AAI UI (sparky-fe)	Mot	Met	Met	Mac	Mat	(Max)	NA NA	Clonat	ONAP AAI UI (sparky-fe)	Unna		Mat	Met	Met	Max	Mac Mac	Ma	ONAP AAI UI (sparky-fe)	MA
ONAP Active and Available Inventor ONAP APPC	<u> </u>	(Mar)	Mod	(Mat)	Met	we	Met	Met	(Mac)	Mat	ONAP Active and Available Inventor ONAP APPC	ý 100E	(MI)	(ME)	Met	Needs URL	INK	Needs UPC	(Ma)	Met	Nat	ONAP Active and Available Inventory ONAP APPC	Mar Mar	.7	(Met)	Mot	Wat	(Max)	met III	Mut	ONAP Active and Available Inventory ONAP APPC	Uronal	ii (Me	(Mell)	(Mar)	(MI)	I Mari	MK MK	Max	ONAP Active and Available Inventory ONAP APPC	INK!
ONAP APPC (Application Controller)		- War	Mod	Met	Met	Met	Met	Met	Mac	Unnat	ONAP APPC (Application Controller)	- Marie	Met	(Mar)	Met	Unit	Mat	Mat	Mer	Met	Vet	ONAP APPC (Application Controller)	Met	Met	Met	Met	(Vat.)	Mar Mar	Max Max	Mut	ONAP APPC (Application Controller)	l Mar	(Mar)	Matt	Met	(Met)	Mot		Unmet	ONAP APPC (Application Controller)	Unnet
ONAP CCSDK (Common Controller SDK)	7	(WZ)	Báse	(Mar)	Met	Met	Met	Met	(Me)	Met	ONAP CCSDK	1	(Mel)	(W)	Met	Met	NA.	Needs UPC	(Met)	Met	Mat	ONAP CCSDK	Met Met	INAI	(Met)	that	(Mat)	(Max)		Mat	ONAP CCSDK	Unmat	(Mac)	(Mat)	(Mar)	(Met)	bloc	Mac Mac	Mar	ONAP CCSDK	INA.
Controller SDK) ONAP Champ	-	w	Mor	(Me)	Met	Met	Met	Met	(Me)	Mat	(Common Controller SDK)	-	(Me)	(Mr)	Met	Noods UPC	INKI	Noods UPC	(Me)	Met	Vat	Controller SDK) ONAP Champ	Mat Mat	Met	(Mt)	Mot	- Wat	(Max) (Us	mat) [2]	INKI	Controller SDK) ONAP Champ **	Uhrea		(Met)	(Met)	(Met)	Max	Mac Mac	Max	ONAP Champ	Met
ONAP DCAE	, Mari	We	3	Mut	Met	7	1 11	IN/X	(Mac)	Met	ONAP DCAE	· we	Met	Ma		171	Mat	Met	Mil		121	ONAP DCAE	Mar Mar	Met	(Met)	Met	(Max.)	(Nac)	NA I	Mix		Unred	i Mar	Mel	Mat	Met	Unnet	Mac Mac	RA.	ONAP DCAE	INA
ONAP DMaaP Buscontroller	· ·	We		Mer	Met	2	Met	Met	(Me)	Net	ONAP DMssP Buscontroller	/ <u></u>	(Ma)		Met	181	INKI	Wet	Me	Unnet	Max	ONAP DMssP *	Met Met	Met	Met	Met	Mat	(Mar)	INAI	Net	ONAP DMaaP Buscontroller	Unma	ii wa	Met	(Met)	Met	Mut	Mac Max	INA	ONAP DMssP -	INA
ONAP DMaaP Data-Router	- (Met)	(W)	Unnet	Met	Met	INAI	Met	Met	(44)	Mel	ONAP DMaaP Data-Router	-	(MI)	(W)	Met	No.	INAI	TWF	(M)	Mel	Nat	ONAP DMaaP Data-Router	Mari Mari	Met	(Mel)	Mel	Mat	(Net) (Ne			ONAP DMaaP *	i wai	(Mar)	Mel	(800)	(MI)	Mat	Mat Mat	INKI	ONAP DMaaP Data-Router	. INAI
ONAP ESR (External System Register)	· (we)	(Wa)	Met	(Mat)	Met	Met	Met	Met		Net	ONAP ESR (External System Benister)	1	(MI)	(Wa)	Met	IN	Urmet	Needs UTC	(MI)	Met	Wat	ONAP ESR (External System	Mari (Mari	INA	(Mil)	TAN	(Vit)	(Me)		Mel	ONAP ESR (External System	Unrel		(Mel)	Met	(MI)	Met		Useset	ONAP ESR (External System	Me
ONAP External			7	Met	7	7		INA		2	ONAP External	-				100	NA I	171			121	ONAP External **		<u></u>			(Mat.)		-	Mil	ONAP External **		Met			20	Mat	10	10	ONAP External *	
ONAP Gizmo	· ·	(Ma)	Mil	(Mar)	Mer	Mil	Met	INAI	(Mar)	Mat	ONAP Gizmo	4 100	(MI)	(Wa)	Met	100	INKI	Noods UPC	(Mar)	Mer	Vat	ONAP Gizmo	Mar Mar	NA	(MI)	tion	(Mat)	(Max) (Un	nat)	NA.	ONAP Gizmo **	Unrel		Mel	(Met)	(MI)	Mac	Mac Mac	164	ONAP Gizmo	[MK]
ONAP Holmes	•	(Ma)	-	(Mat)	Met		-	INAI	(Me)	-	ONAP Holmes	-	(Mil)	(Mr)	Met	-	INK	Net			Met	ONAP Holmes				-	Wat	· · · · · · · · · · · · · · · · · · ·	NA.	Met	ONAP Holmes *		Met				I MARI	D E	7	ONAP Holmes	m
ONAP Model Loader	· •	w	Mot	Mat	Met	Met	Met	Met	Me	Mat	ONAP Model Loader	· we	Met	(Mat)	Wet	Met	INKI	Noods UPC	Met	Met	Vat	ONAP Model Loader	Mot Mot	INAI	Met	Met	Wat	Mar Us	net 1	Mat	ONAP Model **	Uhrmal	ii wa	Mati	Met	Met	Made	Mac Mac	Mar	ONAP Model Loader	NA.
ONAP Modeling ONAP Operations Manager	· •	w	INNI	Met	Met	Unveil	Met	INAL	(Max)	Met	ONAP Modeling ONAP Operations Manager	· ·	(Mer	(Ma)		2	NA NA	Umat	(Met)	2	NXII	ONAP Modeling ONAP Operations Manager	Unnet Unne	D INAI	(Met	Unnet	Vit	(Nat) (Us	met Unmet	Met	ONAP Modeling * ONAP Operations * ONAP Operation	met Unmet	(Mar)	(Met)	Unmet	Urrset	INAI (Nuc Nuc	INA	ONAP Modeling ONAP Operations Manager	INK!
ONAP Optimization Framework (OOF	(Mat)	Wat	Mot	Mat	Met	7	Met	Met	Mac	Met	ONAP Optimization Framework (OOF	Max	Met	Wat	Met	Not	NA.	Met	Met	2	21	ONAP Optimization Framework (OOF)	Met	Met	Met	Met	(Net	(Nat	2	Mut	ONAP Optimization Framework (OOF)	Unmat	ii Mee	Met	Met	Met	Mot	Mac) Mac	Mat	ONAP Optimization Framework (OOF)	NA
ONAP POLICY	· ·	w	Mil	(Met)	Met	Mil	Met	Met	(Me)	Met	ONAP POLICY	· mel	(Mil)	(Ma)	Met	[Met]	Val	Met	(Me)	Met	Wet	ONAP POLICY	[Mil]	Met	(Mil)	Met	(Vit)	(Me)	i Mari	Met	ONAP POLICY .	D Me	(Mar)	Met	Met	Met	I Mari	Mar) Mar	Unred	ONAP POLICY	Unnet
ONAP SDC (Service Design and Creation)	(Ma)	(Wa)		(Mil)	-	181	-	121	(Mar)	-	ONAP SDC (Service Design and Creation)	-	(MI)	(Ma)	-	7	INK	M	(Me)	2	m .	ONAP SDC (Service Design and Creation)	Met	Met	(Met)	-	(Mat		-	Met	ONAP SDC (Service Design and Creation)		(Mar)	Mel	(Mel)	(Mel)	-	Mit Mit	7	ONAP SDC (Service Design and Creation)	
(SDN Controller)	(000	w	111	(Mat)	Mel	100	Met	[Met]	(Ma)	126	ONAP SDNC (SDN Controller)	1 ==	(MI)	(Wa)	31	181		IMI	(MI)	Mel	12 1	ONAP SDNC (SDN Controller)	Met Met	Met	(MI)	35	Wat	(MI)		Mil	TODA COMORDI		(Mar)	(Mell)	(Met)	(MI)	1 1	Ми		ONAP SDNC (SDN Controller)	INNE
ONAP SORe	1 000	(W)	Med	(Met)	Unset	No.	Unnet	Wel	(Me)	Met	ONAP Solke	· ·	(MI)	(MI)	Wet	Met	NA.	Wit	(MI)	Unnet	Vet	ONAP Solve	Met Met	Met	(MI)	Mot	(Ma)	(MI)	I MAKE	Met	ONAP Spike * M	Uronal		(Mail)	(Met)	(MI)	Mari (Mar Mar	Unnet	ONAP Solva	Uwul
ONAP Spike ONAP Virtual Infrastructure Deployment (VID)	/ WE		Mot	(Mar)	Met	Net:	- Met	SACE .			ONAP Spike ONAP Virtual Infrastructure Deployment (VID)	1	- Mer		will .	Alactic UPC.	INK!	nelds UFC	-	- ske	-	ONAP Virtual Infrastructure Desturment OUD	Mat Mat	Met	(Met)	SAGE 1	(Mat.)	<u></u>	-	NA.	ONAP Spike (M	Unma	(WE)	Mer	Mer	Mer	nist (Mar. Mar.	not .	ONAP Virtual	
ONAP VNESDK	-		-	(Mat)				Met .		-	ONAP VNFSDK	1			-	121	\vdash	12.			-	Deployment (VID) ONAP VNFSDK				-	Mat			Met	Deployment (VID) ONAP VNFSDK		Mac				Unnet	D D	2	Deployment (VID) ONAP VNFSDK	
ONAP-DMaaP- messagerouter	· ·	w	-	(Met)	Met	-	Met	Met	(Me)	Met	ONAP-DMaaP- messagerouter	· we	(Mil)	(MI)	Met		Vat	Mr.	(MI)	Unet	Vat	ONAP-DMaaP- *	Mar Mar	Met	(Met)		(Mat)	(Max)	D Max	Mat	ONAP-DMaaP- **		Mat	Mati	(Met)	MI	Mar (ми	NA.	ONAP-DMaaP- *	INX
Portal Platform	/ Will	w	Mot	Mar	Met	Unnat	Met	Unit	Mac	Met	Portal Platform	- 100	(Mat)	(Wat)	Wet	Met	INK	Wat	(Mar)	Met	Unnat	Portal Platform *	Met Max	Met	(Met)	Met	Wat	(Max) (Us	met Unmet	Mat	Portal Platform *	Unma	i Mar	Matt	(Mat)	Met		Mac Mac	Max	Portal Platform	Unvet
VF-C (Virtual Eunction Controlle Project)			-	(Mar.)	-	100	-	[NA]			VF-C (Virtual Eunction Controlle Project)	1=				2	INK!	191 191				VF-C (Virtual Function Controller Project)		-		-	(Mat.)		-	Mat	VF-C (Virtual Function Controller	=	(ME)				INK	0 2		VF-C (Virtual	
Project)	· Mac	w	Mac	Mat	NA I	INA.	NA.	Met	- Mac	Mat	Projecti vvp	-	(MI)	···	Met	Met	NA.	No.	···	Met	Wat	Project)	Mac Mac	NA.	Met	Mot	Mat	(Max) (Max	i Mari	Mat	Project)	in the	Mac	Mati	Mac	(Met)	Mac	Mac Mac	Unnet	Project)	Unveil
rd Name	Code Of Conduct	Coding Standards	Coding Standards Enforced		_		Crypto Verification Private	Crypto Weaknesse	Dependency Monitoring	Documentation Achievements	Name	Documentation Architecture	Documentatio Current	Documentation Quick Start	Documentation Roadmap	Documentation Security	Dynamic Analysis Unsafe	External Dependencies	Governance	Implement Secure Design	Input Validation	Name	Installation Common Ins	allation Installati	Maintenance Or Update	Regression Tests Added50	Report Tracker	Roles S Responsibilities Re	igned Pass leases Sect	es Static Analysi word Common vity Vulnerabilitie	Name M	at Policy Indated Cove	Test Test tement Docum prage80 Add	ts Updateable ented Reused ed Componen		Vulnerability Response Process	Warnings Strict	Dco Bus Factor		Name	Internationalization
								•	•			_	•						•					1									. ,		•						



Thank you

That's all

Q&A

