Information Security Maturity Models Evaluations: Measuring NIST Cybersecurity Framework Implementation Status

IARIA CYBER2021: Manuscript # **80057**

Authors: Alsaleh, Majeed and Niazi, Mahmood
Email: (g198925300; mkniazi)@kfupm.edu.sa

Presented by: Majeed Alsaleh

King Fahd University of Petroleum & Minerals

Professor Mahmood Khan Niazi (mkniazi@kfupm.edu.sa): He received the Ph.D. degree from the University of Technology Sydney, Australia. He has spent over a decade with leading technology firms and universities as a process analyst, a senior systems analyst, project manager, a lecturer, and a professor. He is an active researcher in the field of empirical software engineering. He is interested in developing sustainable processes in order to develop systems that are reliable, secure, and fulfills customer needs. He has published over 100 articles. He has participated in and managed several software development projects. His research interests are evidence-based software engineering, requirements engineering, sustainable, reliable and secure software engineering processes, global and distributed software engineering, software process improvement, and software engineering project management.

Majeed Alsaleh (majeed.saleh@mail.com): He received B SC. Degree in Computer Engineering from King Fahd University of Petroleum & Minerals (KFUPM), Saudi Arabia in 1996. He is security consultant at Saudi Arabian Oil Company. He joined the Company in 2002 and worked as IT Analyst, Information System Auditor, Cyber Security Consultant, and Compliance Specialist. He holds a wide variety of industrial certifications that have a high degree of visibility in the field of Information Security and Assurance including CISM, CISA, CRMA, CRISC, CGEIT, ISO27001 LI/LA, COBIT5 Foundations, and COBIT5 Implementer.

His research interests include Cyber Security, Information Security, Information Audit and Assurance.

Outline

- Introduction
- What is the Issue?
- Contributions
- Analysis
- Conclusion
- Future Work

Introduction

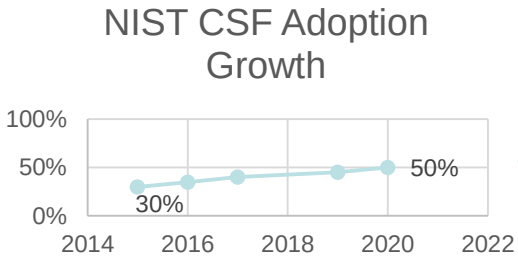
NIST National Institute of Standards and Technology

2014

2013

Gartner

2015



2017

Introduction (Cont.)

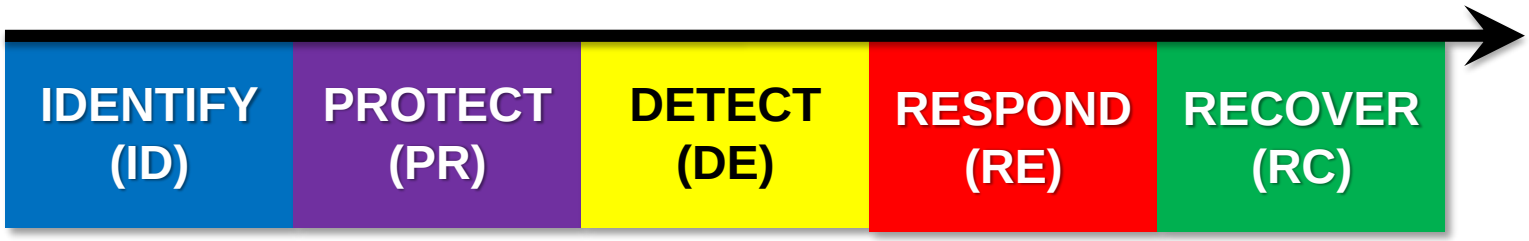
NIST National Institute of Standards and Technology

2018

Version	Functions	Categories	Sub-categories	Informative References
V1.0	**5**	**22**	**98**	**5**
V1.1	**5**	**23**	**108**	**5**

Table 1: Framework Versions Comparison

NIST CSF (Framework Core)



NIST CSF Functions [5]

NIST CSF

PROTECT [6]

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

PR.AC Access Control
PR.AT Awareness and Training
PR.DS Data Security
PR.IP Information Protection Processes and Procedures
PR.MA Maintenance
PR.PT Protective Technology

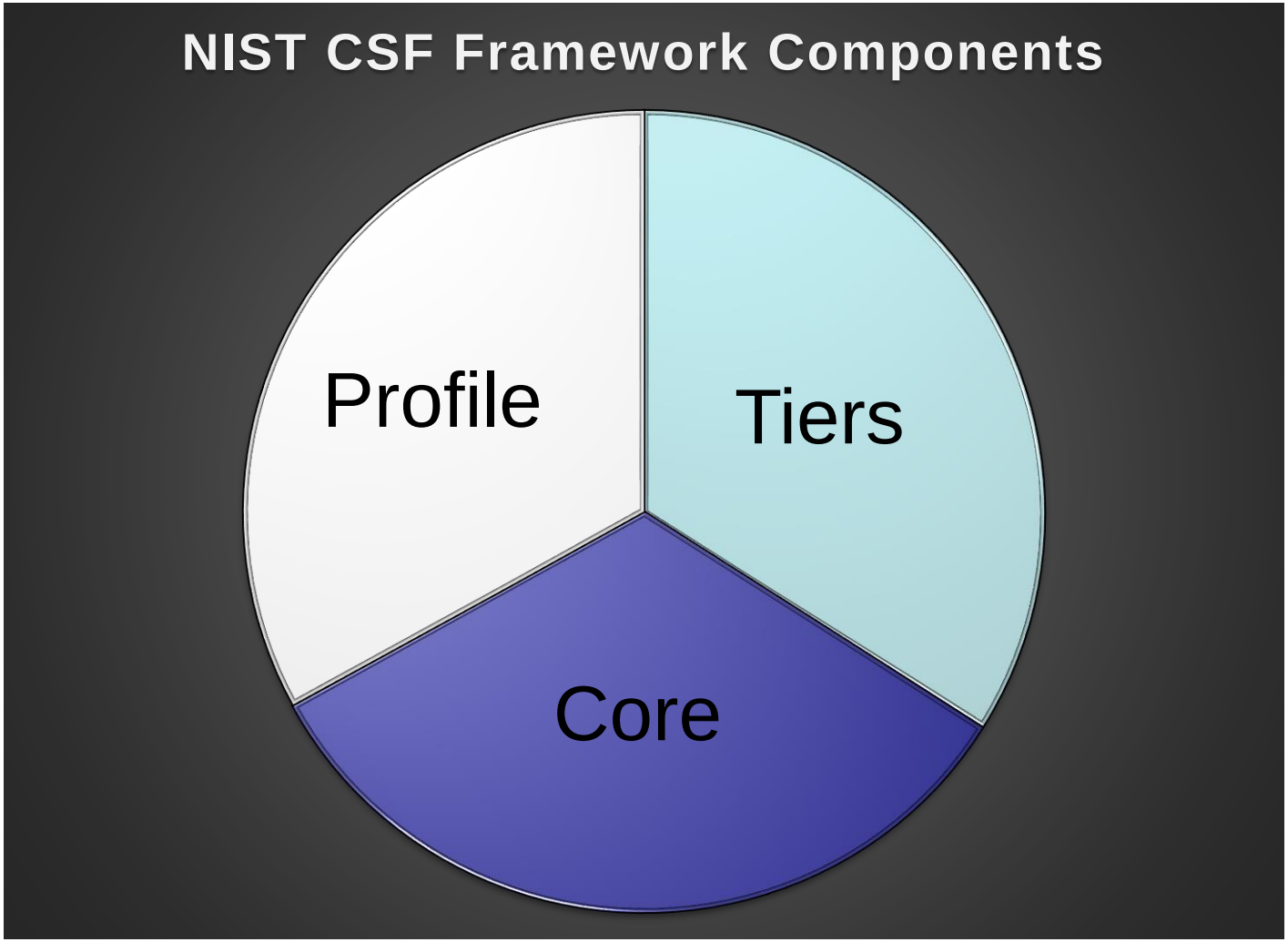
NIST CSF Functions [5]

Examples of sub-categories of the NIST CSF framework

Function	Category	Sub-Categories
Protect	(PR.DS) Data Security	PR.DS-1: Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

Examples of sub-categories of the NIST CSF framework

Introduction (Cont.)



What is the Issue?

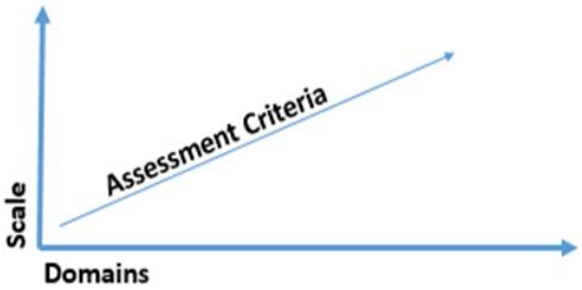
- Verities of available capability maturity models
  - Which one to use?
  - Must be used all the way to measure the progress
  - Is Benchmarking possible?

Contribution

This research main objective is to identify and apply evaluation criteria,

- through reviewing number of existing maturity models,
- seeking Subject Matter Experts' feedback to define their proposed criteria

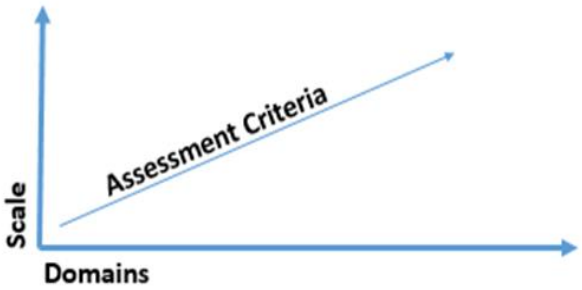
Analysis (CMMs Review)



Levels/ CMM	Level 1	Level 2	Level 3	Level 4	Level 5
SSE CMM	Performed Informally	Planned and Tracked	Well Defined	Quantitatively Controlled	Continuously Improving
PAM	Performed Process	Managed Process	Established Process	Predictable Process	Optimizing Process
ISF	Performed	Planned	Managed	Measured	Tailored
CMMI	Initial	Managed	Defined	Quantitatively	Optimizing Managed
CCSMM	Initial	Established	Self-Assessed	Integrated	Vanguard
ISM3	Undefined	Defined	Managed	Controlled	Optimized
ONG	Performed but Ad-hoc	Defined and Resourced	Governed and Effectively Resourced	N/A	N/A

CMMs Levels Comparison

Analysis (CMMs Review)



Assessment Criteria

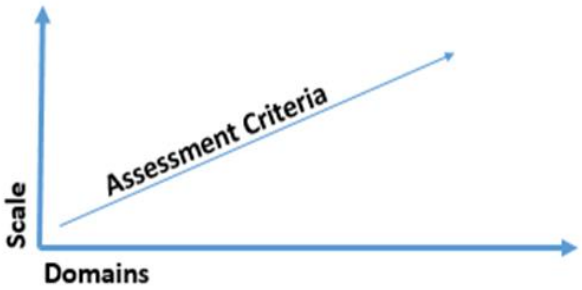
1. **Generic**
2. **Specific**

5. Optimized	for a **high investment** in ISM processes that are managed to result in a highest risk reduction with **compulsory use of process metrics**
4. Controlled	for a **high investment** in ISM processes that are managed to result in a highest risk reduction
3. Managed	for a **significant investment** in ISM processes that are managed to result in a highest risk reduction
2. Defined	for a **moderate investment** in ISM processes that are managed to result in a further risk reduction
1. Undefined	for a **minimum investment** in essential ISM processes that are managed to result in a significant risk reduction

Levels\ Categories	GP 1	SSP1 . . . SS P6	TSP1 . . . TSP 111	OSP 1. . . . . OSP2 5
	General	Strategic Management	Tactical Management	Operational Management

ISM3 criteria to verify the process capability maturity

Analysis (CMMs Review)



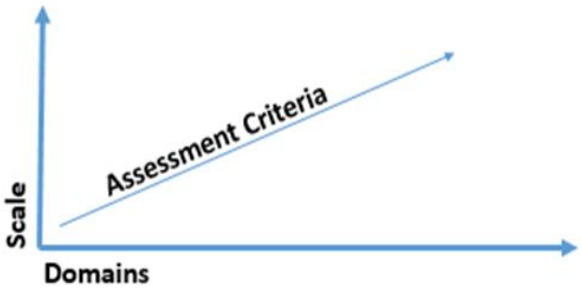
Assessment Criteria

1 **Generic**

2 **Specific**

5. Optimizing	1 Process innovation 2 Process optimization				
4. Predictable	1 Process measurement 2 Process control				
3. Established	1 Process definition 2 Process deployment				
2. Managed	1 Performance management 2 Work product management				
1. Performed	1 Process performance				
0. Incomplete	No attributes				
Levels\ Categories	Evaluate, Direct and Monitor	Align, Plan and Organize	Build, Acquire and Implement	Deliver, Service and Support	Monitor, Evaluate and Assess
PAM criteria to verify the process capability maturity					

Analysis (CMMs Review)



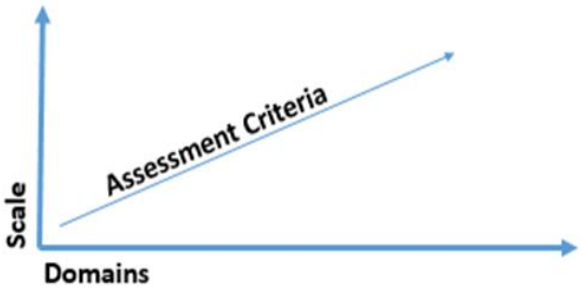
Assessment Criteria

1 Generic

2 Specific

5. Tailored	The activity is performed, planned, managed, measured, and subject to continuous improvement and is tailored to specific areas																		
4. Measured	The activity is performed, planned, managed, and is monitored																		
3. Managed	The activity is performed, planned, and has sufficient organizational resources to support and manage it																		
2. Planned	The activity is performed, and supported by planning (which includes engagement of stakeholders and relevant standards and guidelines)																		
1. Performed	The activity is performed																		
0. Incomplete	The activity is not performed																		
Levels\	D1	D2	.	.	D6	D7	.	.	D12	D13	D14	D15	.	.	.	D19	D20	D21	
Categories	Strategic				Technical				Connections			Crisis					People		
ISF MM criteria to verify the process capability maturity																			

Analysis (CMMs Review)



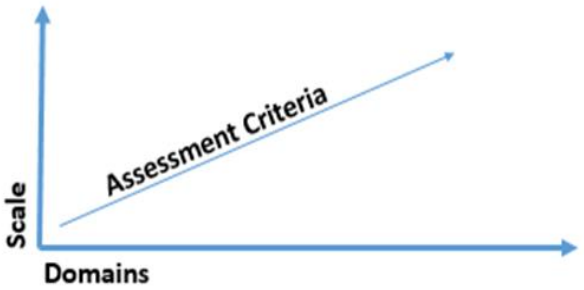
Assessment Criteria

1. **Generic**
2. **Specific**

5. Continuously Improving	Improving Organizational Capability
4. Qualitatively Controlled	Establishing Measurable Quality Goals Objectively Managing Performance
3. Well Defined	Defining a Standard Process Perform the Defined Process Coordinate the Process
2. Planned and Tracked	Planning Performance Disciplined Performance Verifying Performance Tracking Performance
1. Performed Informally	Base Practices are Performed
0. Not Performed	No process is performed
Levels\ Categories	PA 1 . . . . . PA 11 PA12 . . . . . PA22 Security Engineering Process Areas / Project and Organizational Process Areas

SEE CMM criteria to verify the process capability maturity

Analysis (CMMs Review)



Assessment Criteria

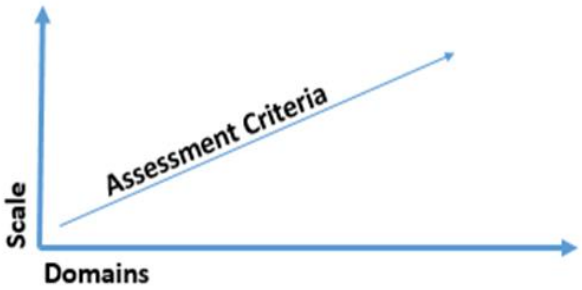
1 Generic

2 Specific

5. Optimizing	1. Causal Analysis and Resolution 2. Organizational Performance Management
4. Quantitatively Managed	1. Organizational Process Performance 2. Quantitative Project Management
3. Defined	1. Decision Analysis and Resolution 2. Integrated Project Management 3. Organizational Process Definition 4. Organizational Process Focus 5. Organizational Training 6. Product Integration 7. Requirements Development 8. Risk Management 9. Technical Solution 10. Validation 11. Verification
2. Managed	1. Configuration Management 2. Measurement and Analysis 3. Process and Product Quality Assurance 4. Project Monitoring and Control 5. Project Planning 6. Requirements Management 7. Supplier Agreement Management
1. Initial	no process area is performed
Levels\ Categories	PA1 . . . . . PA11 PA12 . . . . . PA22
	Process Management / Project Management / Engineering / Support

CMMI criteria to verify the process capability maturity

Analysis (CMMs Review)



Assessment Criteria

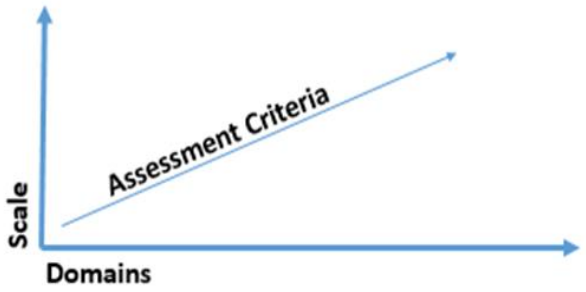
1 Generic

2 Specific

5. Vanguard	Awareness is a mandatory by the business	Fully integrated	Full-scale combined exercises and assess complete fusion capability	Continue to integrate cyber in COOP
4. Integrated	Leaders and organizations promote awareness	Formal information sharing internal and external to the community	Self-directed cyber exercise with assessment	Integrate cyber in COOP
3. Self-Assessed	Leaders promote awareness	Formal local information sharing	Self-directed tabletop cyber exercise with assessment	Include cyber in COOP; formal cyber incident response/recovery
2. Established	Leadership aware of cyber threats…	Informal Information sharing	No assessment but aware of requirement	Aware of need to integrate
1. Initial	minimal cyber awareness	minimal information sharing capabilities	minimal cyber assessments and policies evaluations	Little inclusion of cyber in the community's Continuity of Operations Plans (COOP)
Levels\ Diminutions	Awareness	Information Sharing	Policies	Plans

CCSMM criteria to verify the cybersecurity maturity

Analysis (CMMs Review)



Assessment Criteria

1 Generic

2 Specific

Manage Asset Configuration	
MIL1	Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly
	Configuration baselines are used to configure assets at deployment
MIL2	The design of configuration baselines includes cybersecurity objectives
MIL3	Configuration of assets are monitored for consistency with baselines throughout the assets' life cycle
	Configuration baselines are reviewed and updated at an organizationally-defined frequency
Examples of evaluation criteria for ONG C2M2 objectives	

Analysis (Survey Design and Analysis)

Interviewed SMEs,

- cybersecurity,
- information security management,
- information systems audits, and
- internal control management

Analysis (Survey Design and Analysis)

16 questions and twelve cybersecurity professionals responded to the survey

- 58% of the participants are GRC specialist (distributed as 25% Compliance specialist, 17% as Governance, and 17% as Risk specialist).
- 25% of the participants were senior information systems auditors.
- 8% of the participants were compliance officers
- 8% were process performance assessors.

Analysis (Survey Design and Analysis)

Q1: Does your Organization adopt NIST CSF or planning to?

- 75% Yes
- 25% are planning to adopt the framework.

Q2: Are there any governance requirements mandate to adopt NIST CSF?

- 66% are adopting or planning to adopt the framework
- 34% are voluntarily adopting the framework.

Q3: How many times you assessed your organization maturity

- While all organizations assessed their cybersecurity maturity at least once, more than 58% did the assessment t more than three times.

Analysis (Survey Design and Analysis)

Q4: Did you use the same CMM in all assessments?

- 75% used the same CMM for the assessment
- 25% used different CMM.

Q5: Did you use or plan to use the result for Benchmarking?

- 90% of the organizations either used the result of the assessment or planning to use it for benchmarking with other organizations in their field of operation.

Q6: Did you use or plan to use CMM to certify your organization?

- Including the certification as part of the assessment goals was the intent of 50% of the organizations.

Analysis (Survey Design and Analysis)

Q7: What is your preference related to training?

- More than 90% of the organizations preferred that the selected maturity model provides training in various formats including the in-class.

Q8: Did you use or prefer to use a CMM linked to a framework?

- 75% Yes
- 25% No-Preferences

Q9: Did you use or prefer to use CMM that is mapped to NIST CSF Functions/categories/sub-Categories?

- 75% Yes.

Analysis (Survey Design and Analysis)

Q10: Do you prefer the mapping done by NIST or the CMM owner?

- More than 66% of those organizations want the mapping done by NIST in specific as part of the informative references.

Q11: What is the level of the mapping you prefer?

- 66% of the organizations prefer “One-to-One” mapping,
- 25% prefer “Close to One-to-One” mapping,
- 9% have no preferences

Analysis (Survey Design and Analysis)

Q12: What is the Scale levels you used or prefer to use?

- More than 83% of the organizations preferred to use a CMM of five levels scale.

Q13: Do you prefer to use the description of the scales levels as is or you modify it?

- More than 66% of organizations preferred to use the description of the scales levels as is, while the remaining preferred to modify it.

Analysis (Survey Design and Analysis)

Q14: Did you use or prefer to use Generic criteria or specific criteria to assess each domain in each level?

- 83% of the organizations preferred to use generic criteria to assess each domain in each level.
- 17% preferred to use specific criteria to assess each domain in each level.

Analysis (Survey Design and Analysis)

Q15: Did you use or prefer to use Assessment Criteria that allow different weight for the assessed process/activity?

- 66% organizations used or planning to use assessment criteria that allow different weight for the assessed process/activity.
- 16% are not preferring to use criteria that allow different weight,
- 16% the same percentage of organizations has no preferences against the weight.

Analysis (Survey Design and Analysis)

Q16: What is the scoring preference to use?

- 50% of the organizations preferred the use of cumulative scoring
- 25% of the organizations preferred to use non-cumulative,
- 25% of the organizations preferred to use combined (Non-cumulative for compliance and cumulative for performance).

Conclusion

CMM/ Evaluation Criteria	SSE	PAM	ISF	CMMI	CCSMM	ISM3	ONG
Certification	✗	✗	✗	✓	✗	✓	✗
Training in various formats including the in-class	✓	✓	✓	✓	✓	✓	✓
linked to a framework	✗	✓	✓	✗	✗	✓	✗
mapped to NIST CSF Functions/categories/sub-Categories	✓	✓	✓	✗	✗	✓	✗
mapping done by NIST	✗	✓	✗	✗	✗	✓	✗
“One-to-One” mapping	✗	✗	✗	✗	✗	✗	✗
Five levels scale	✓	✓	✓	✓	✓	✓	✗
Generic criteria to assess each domain in each level	✓	✓	✓	✗	✗	✓	✗
Weighted value for each control	✗	✗	✗	✗	✗	✗	✗
Cumulative scoring methodology	✓	✓	✗	✓	✓	✓	✓

Evaluation criteria and its value versus each CMM

Future Work

- The identification of what CMM is making the top quadrant in practical life.
- Review of case studies for organizations implanted NIST CSF.
- Assess the possibility of one-to-one mapping of NIST CSF to other frameworks or domains of capability maturity models.

Thank You !